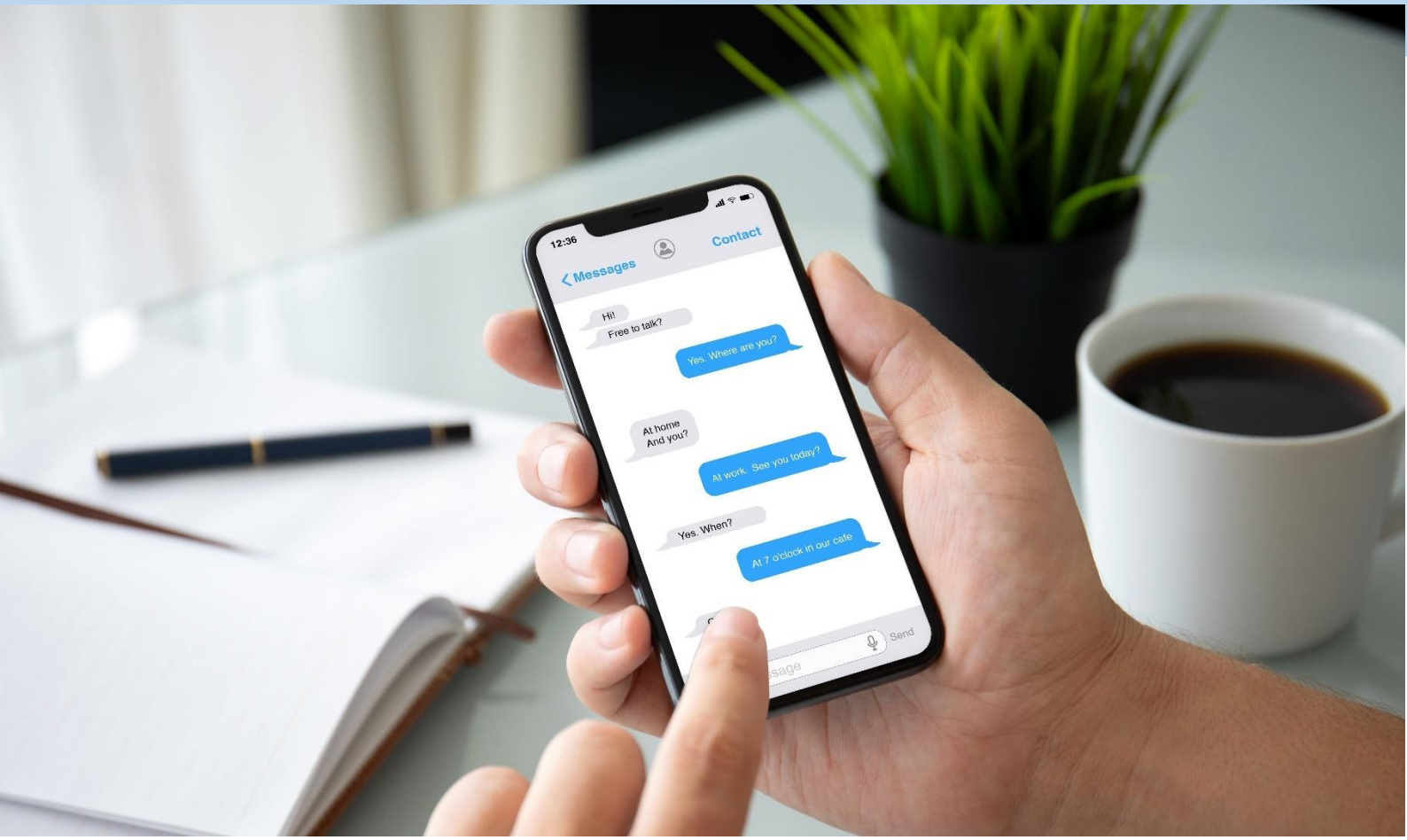
Bundeskartellamt

Offene Märkte | Fairer Wettbewerb

Sector enquiry

Messenger and video services

Final report



Sector enquiry into messenger and video services
Report pursuant to Section
32e GWB Ref. V-28/20
May 2023

Contact
Federal Cartel Office
Decision Division Competition and Consumer Protection
Kaiser-Friedrich-Straße 16
53113 Bonn
www.bundeskartellamt.de

Photo credits:
AdobeStock/DenPhoto

Preliminary remark

In November 2020, the Bundeskartellamt's Competition and Consumer Protection Decision Division initiated a sector enquiry under consumer law pursuant to Section 32e (5) of the Act against Restraints of Competition[1] in the sector of messenger and video services.[2] In November 2021, the interim report "Industry overview and mood picture" was published.
Interoperability", the results of which are also part of this final report.[3] Sector enquiries are not directed against specific companies, but serve to investigate a sector of the economy with regard to possible violations of consumer law.
This was preceded by the first-time transfer of competences in the area of consumer protection to the Bundeskartellamt with the 9th amendment to the Act against Restraints of Competition (GWB), which came into force in June 2017.[4]
Reference is made to the provision of Section 32e (6) GWB on the excluded reimbursement of expenses in the event of a warning pursuant to Section 12 (1) sentence 2 of the Unfair Competition Act[5] (UWG).

---

1 Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen) in the version promulgated on 26 June 2013 (Federal Law Gazette I p. 1750, 3245), last amended by Art. 2 Act of 19 July 2022 (Federal Law Gazette I p. 1214) - GWB.

2 See *Bundeskartellamt*, press release of 12.11.2020, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_SU_Messenger_Services.html?nn=3591568.

3 See *Bundeskartellamt*, press release of 04.11.2021, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2021/04_11_2021_SU_Messenger-Dienste_Zwischenbericht.pdf? blob=publicationFile&v=2.

4 See *Bundeskartellamt*, press release of 12.06.2017, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2017/12_06_2017_Abteilung%20V.pdf? blob=publicationFile&v=2 .

5 Act against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb) as amended on 3 March 2010 (BGBl. I p. 254), last amended by Article 20 of the Act of 24 June 2022 (BGBl. I p. 959) - UWG.

Table of contents

List of figures

Summary

Guiding question of the study

Messenger and video services have become an indispensable part of everyday communication for many people. Consumers can exchange text and voice messages as well as files and make phone calls (via video) on various end devices and use and combine all these functions individually. Long established modes of communication thus appear in a modern guise. The **desire for individuality or a customised solution** for one's own needs is reflected in messenger and video services in a great **variety of business models and applications.** As the Bundeskartellamt has already explained in the interim report on this sector enquiry, the functions, the offers and the economic significance of messenger and video services are very diverse. In addition to the services that are particularly well known to the public, there is a wide range of industry participants, ranging from international, group-operated services with many millions of users, high turnover and their own digital ecosystems[6] with strong positions in neighbouring markets, to national services or services concentrated in German-speaking regions or services with a special business focus, to open source services and free applications without the intention of making a profit. It is a globally active industry that generates technological and digital developments and innovations not only on the part of the larger participants. Competing services are characterised by

---

[6] The term "digital ecosystem" refers to a bundle of a multitude of services of a group with interactions among each other, cf. *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25 April 2022, available at: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf as well as *Bundeskartellamt*, The Evolving Concept of Market Power in the Digital Economy - Note by Germany, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/OECD_2022_Competition_Committee_Concept_Market_Power_Digital_Economy.pdf?_blob=publicationFile&v=2. See also e.g. *Fletcher,* Digital competition policy: Are ecosystems different?, Note for the OECD Hearing on Competition Economics of Digital Ecosystems, available at: https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf. In information technology, the term ecosystem is used to describe a software and hardware architecture, each of which is based on its own devices, systems and access requirements and thus presupposes and generates corresponding accessories, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/%C3%96kosystem.

innovative business models and specialisations based on special services and functions. It is not only on the side of the free systems and applications that there is a lot of expertise and commitment in terms of independence and protection of users' personal data. However, the state of the market suggests that this potential has not yet been exploited, has not been distributed across the board and has not been used to the benefit of a high level of data protection as it could be. This has raised new **consumer law issues.** However, consumers themselves seem to put these consumer law aspects at the back of other criteria when choosing their messenger and video service. Therefore, this final report on the sector enquiry into messenger and video services focuses on the key question of how **data protection** can be advanced **as a competitive parameter in order** to achieve a higher level of data protection in messenger and video services market-wide. What incentives and measures are necessary so that consumers also choose their messenger and video services according to their data protection friendliness? And how can the messenger and video services be persuaded to increasingly use data protection friendliness as a differentiating feature and to better inform consumers about it?

The Bundeskartellamt first examined the initial situation regarding data security and data protection and the competitive environment of the industry. One focus was on the technical foundations and methods of messaging and audio/video exchange. The technical conditions and practices in the individual services not only influence **data security and the (legally compliant) implementation of data protection measures**. The technical infrastructure can also have an impact on competitive processes. It is therefore also decisive for the Bundeskartellamt's goal of promoting data protection as a competition parameter.

It depends, for example, on whether and to what extent it is possible to access and connect to other messenger and video systems or to integrate technical innovations into a system. The complexity of the technical infrastructure and procedures is also likely to affect consumers' initiative. Their willingness to use data protection as a selection criterion as described above first requires a basic understanding of the demanding technical interrelationships. The consumers**' perspective** is crucial for any recommendations for action. Framework conditions must be created and incentives set to motivate them and the services offering them to give data protection a higher priority in competition.

The Bundeskartellamt interviewed more than 40 different services on these topics and conducted a number of expert discussions. In addition, a large number of studies and specialist articles were evaluated.

Course and further topics

In the **interim report,** which was published in November 2021, the Bundeskartellamt presented the results of its investigations in two subject areas: Firstly, an overview of the framework conditions of the **industry** as well as the different provider groups, functionalities and business models was given. On the other hand, the first results of the company survey on **interoperability were** presented. It was questioned to what extent such interoperability would influence data security and thus the level of data protection of messenger and video services and to what extent effects on incentives for innovation and the intensity of competition in the industry are to be expected.

In this **final report,** the Bundeskartellamt has expanded the aforementioned statements to include the findings on the subject of data protection in messenger and video services, in particular **data security and data processing criteria.** The results of the investigations are presented, classified and legally reviewed. Furthermore, the results of the investigation on **interoperability**, which have not yet been published, are presented and related to the corresponding regulations of the **Digital Markets Act (DMA),** which has meanwhile come into force on 1 November 2022. Against this background, **approaches for more competitive data protection are** developed, which are directed at both consumers and services. Building on this, the report concludes with **recommendations for** improving the level of data protection in messenger and video services in Germany. Here, not only the legal conditions, tendering and funding practices and the situation of the public sector are addressed. It is suggested to improve the **framework conditions for competitive data protection and to** introduce a transparent evaluation of data protection quality.

Data security and data processing criteria for messenger and video services

For this sector enquiry, the Bundeskartellamt has dealt in detail with the technical foundations of messaging and audio/video exchange. It has drawn up a **checklist** with the essential criteria for data security and data protection. This first covers the **protocol** including end-to-end encryption on the state of the art. The protocol can be understood as the language of a messaging and video system that includes the rules for exchange and connection to the system. **End-to-end encryption** ensures that the data exchange from sender to receiver cannot be read by anyone other than the communicators themselves. Encryption only makes sense if the identity of the users exchanging the encrypted data is also unique. With **two-factor authentication,** consumers can confirm their own identity to their

Messenger and video service as well as to their communication partners.

If services generally use **international technical standards,** this goes hand in hand with a certain verified level of quality. In addition, interoperability can be established more easily if communication is based on identical technical principles. If the **source code of a messenger and video service is accessible**, competent third parties can check the data security of the system. If this is not the case, there should be the possibility that at least security audits are carried out and published by independent renowned testing institutions. Unless the privacy policy is read, the nature of the business model can be an indication of whether or not data will find uncertain further use. Here, attention should be paid to **data economy.** If users have to create **accounts,** as is the case with services of large corporations that operate a digital ecosystem, a lot of data is already collected through this.

Messenger and video services should **store** EU citizens' data **within the scope of the GDPR** and not transfer it to other jurisdictions in order to maintain data security in compliance with the law. This concerns in particular the comparison with the USA, where intelligence services can access consumer data stored there. Consumers can protect their data and that of their contacts if they **refrain from** synchronising the **contact directory or** select or instruct their service accordingly.

The results of the investigation had to be evaluated according to several standards. First, it had to be checked whether the criteria of data security and data protection were implemented according to the **state of the art and whether they** were sustainable. This question became more important against the background of possible interoperability of messenger and video services and their impact on data protection and data security. Shortly before the conclusion of the sector enquiry - in November 2022 - the DMA came into force with an **interoperability regime** for gatekeepers, which concretised the legal environment on this issue. Finally, **consumer perceptions** had to be included. Various consumer surveys and scientific studies do not allow any clear conclusions to be drawn as to the extent to which consumers are able and willing to work out complex technical backgrounds and translate them into privacy-friendly selection strategies. Also, whether and to what extent the **information and presentation of data protection-relevant facts** by the services is suitable for **informing** consumers. "capture" is questionable. Doubts seem to exist here in view of the current state of the market and the The strong position of well-known services continues to be appropriate.

According to the result of the investigation, much exists in the messenger and video services industry. **Innovative strength and expertise** in matters of independence and protection of the personal data of the

users. However, at the same time, **various practices are to be criticised in** the sector. The findings of the sector enquiry suggest that various services lack commitment and do not implement expertise and opportunities as would be desirable and possible from the users' perspective. However, this is difficult to pin down to individual groups of services. For example, according to the results of the investigation, free messaging systems and open source services score well on a large number of the criteria. However, the question of how data security is designed in detail ultimately depends on the selected (server) operator. In general, most services offer users **many choices**, some of which require a certain awareness of security-relevant actions, such as - as just mentioned - the **selection of the server operator** or, in general, the **activation of end-to-end encryption**. Conversely, if consumers are willing to inform themselves, they can find a **wide range of options for** designing their messenger or finding the client that best meets their requirements and is also future-proof in terms of interoperability due to data economy and the use of international standards.

Some videoconferencing services also offer their users many options. To a large extent, this is due to the orientation towards the wishes of business customers. A high level of security can be implemented. Ultimately, however, security-conscious action is often the **responsibility of the respective host** or administrator, regardless of whether this role is performed for business or private purposes.

As far as the practices to be criticised or the lack of commitment are concerned, this concerns **encryption on the one hand**. Individual well-known messenger and video services surprise with the fact that they do **not** implement state-of-the-art security and, for example, leave it at transport encryption or only use end-to-end encryption for certain functions, which cannot be justified with technical restrictions. Furthermore, it would be desirable that other security procedures, such as encryption of data on the end device, filing encryption, two-factor authentication and backups, had a higher degree of diffusion in the industry. Furthermore, reference should be made to the legal analysis. Some services **store data of European users outside the scope of the GDPR**, which is not legally permissible**,** or the exact storage location remains unclear. The **synchronisation of the contact directory as a** result of which third party data is processed is also operated by various services and may be inadmissible.

Legal classification

The Bundeskartellamt initially requested information from the messenger and video services on data storage and data transfer as well as on the synchronisation of the contact directory and subjected the results to a legal analysis. According to the results of the investigation, **some messenger and video services** appear to have **violated** the provisions of the GDPR.

The **synchronisation of the contact directory** leads to the contact data of non-users also being recorded. In the Bundeskartellamt's current view, this common practice of many well-known messenger and video services does not meet the requirements of Art. 6 (1) subpara. 1 a) DSGVO, provided it is permanent. The personal reference of the data persists even if the telephone number is replaced by a cryptographic hash value linked to the user from whose contact directory the telephone number originates. No further legitimisation of the data controller results from the protection of legitimate interests, as the networking advantage appears too small.

The results of the investigation into the data processing process suggest that some messenger and video services do not behave in a legally compliant manner when **transferring data to third countries and storing it on servers in third countries** (Art. 45 GDPR). This primarily concerns those services that store data of German users in the USA. Data may only be transferred to countries outside the EU and the European Economic Area if an adequate level of data protection is ensured in the respective third country (Art. 45 DSGVO). However, the former data protection shield (EU-US Privacy Shield), which the EU had negotiated with the USA, has been terminated after the
"*Schrems II*" - ECJ ruling from summer 2020 invalid.

In addition to possible violations of the GDPR, another legal field of investigation was a possible misleading of consumers due to **information deficiencies (**Section 5a (1) UWG) **in end-to-end encryption**. Here, in the Bundeskartellamt's view, a transparency violation due to information deficiencies regarding the type of encryption should not be easy to justify. For a possible violation of the transparency requirement of the UWG, the
"business relevance" of security features such as end-to-end encryption can be justified. However, market development has progressed since the conception of the sector enquiry. End-to-end encryption has established itself as an industry standard, so it should make no difference where users register with regard to this security feature. Against this background, it was surprising that a few well-known services do not implement end-to-end encryption at all or only to a limited extent. A better assessment of the consumer's perspective would have provided further information on the security of end-to-end encryption.

This would have required an investigation effort such as a consumer survey, which would have had only uncertain chances of clarification due to the complexity of the terms. The classification of the consumers' behaviour from the company's point of view also remained ambiguous, as there are many free offers of messenger and video services. Ultimately, a conclusive assessment had to be left to **clarification in** each **individual case.**

Interoperability

With the entry into force of the Digital Markets Act in November 2022, the legal environment of messenger and video services in terms of interoperability has been clarified. Due to the ongoing legal policy discussion on a legal obligation of messenger and video services to interoperability, the Bundeskartellamt had **already asked** the companies surveyed questions on this complex of topics in its investigation **before the agreement in the trilogue on the DMA in March 2022.** As already explained in detail in the interim report, the Bundeskartellamt's questioning of the companies had a clear focus. The aim was to follow up on the variously expressed expectations that interoperability would facilitate the switch to data protection-friendly messenger services and thus promote **data protection quality** in this area. Other objectives associated with interoperability, such as ensuring connectivity in the area of interpersonal communication or reducing the market power of leading messenger services, were not the direct subject of the investigation.

According to the results of the investigation presented in the interim report, the technical requirements, the design of data security, the interactions of interoperability with regard to innovation incentives and the intensity of competition, as well as consumer behaviour, could be seen as significant **influencing factors for data** protection effects through interoperability. Overall, the survey had shown that interoperability is not rejected outright by the companies concerned. On the contrary, interoperability or at least forms of exchange are already practised in sub-areas with varying technical depth and scope. Technical foundations for interoperability in a global context are being developed in standardisation committees. However, this was accompanied by the clear position of a large part of the industry that a legal obligation for industry-wide interoperability would do more harm than good and should therefore be rejected. In the case of enforced interoperability, the companies with a negative stance fear in particular negative effects on innovation activity and thus also on the level of data security and data protection in messaging and videoconferencing.

The Bundeskartellamt had highlighted that the findings from the industry survey prove how multi-layered and complex the **analysis of the interdependencies around the topic of interoperability** is. During implementation, not only should the necessary investments in technical

changes in services or the development of technical innovations should be taken into account. Also to be included would be possible positive or negative welfare effects through changed innovation incentives and effects on business strategies and competitive intensity.

According to **the concept of an interoperability obligation standardised in Art. 7 DMA,** only designated gatekeepers among the messenger services are the addressees of the obligation. Furthermore, the obligation only comes into force as soon as another service (voluntarily) approaches the gatekeeper with a corresponding petition. Finally, only the basic functions are covered by the obligation.

Nevertheless, the practical challenges involved are likely to be considerable. Data security must also be technically guaranteed under interoperability. Due to the diverse individual solutions of the services and technical challenges, a **market-wide interoperable end-to-end encryption** remains a challenge so far. In addition, there are numerous data-related difficulties to overcome. This concerns, for example, **data monitoring and accountability** when passed through more hands. With different handling of contact directory and data storage among services, **legally compliant behaviour** must be ensured **at all times.** Whether and to what extent **innovation opportunities** can be preserved is a complex question that cannot be solved theoretically. According to the findings from the investigations, doubts are certainly warranted here. It is true that the DMA interoperability regime is limited to basic functions. However, the architecture of the services and the technical location of the individual functions on it are very individual, so that interoperability here would require standardisation and adjustments to varying degrees, which could also affect the forces of innovation differently.

The assessment ultimately depends on the assumed development scenario. If there were only individual or a few **bilateral agreements** between gatekeepers and petitioners, the challenges would appear to be solvable, especially since the difficulties on the part of the petitioners are accepted voluntarily. A large number of individual reference offers, on the other hand, appears disadvantageous from an overall economic perspective, so that corresponding market-wide standardisations would then have to be discussed. According to the results of the Bundeskartellamt's investigations, the latter seems unlikely at this point in time. It cannot be ruled out that the interoperability obligation for gatekeepers **offers opportunities to new entrants** who are dependent on connection to the large networks of leading services.

Approaches for more competitive data protection

The quality of data protection does not seem to receive the necessary attention within competitive selection processes, especially on the part of consumers as demanders and also for some services. It should therefore not be assumed that the data

will improve the level of data protection under the given framework conditions in a market-driven way. On the contrary, data protection-friendly services must be strengthened in competition. On the other hand, it must be questioned which incentives are necessary so that consumers recognise data protection quality as an essential product characteristic and switch to data protection-friendly services.

Competitors of established services have pointed to **discriminatory tender conditions for** messaging and video services with factually unnecessary hurdles. Here it would be necessary to check which conditions are actually necessary for the desired fulfilment of functions. A less restrictive handling of additional requirements, e.g. size and turnover, could possibly pave the way for data protection-friendly services.

Many of the services interviewed also expect positive effects on the level of data protection from a review of the current **funding practice of open source and standardisation. In** favour of the security of users' data, the entire life cycle of a software could be included. Not only the newly developed application or technology as an innovation, but also the continuous maintenance and care of the products established on this basis on the market and used by consumers appears worthy of promotion in terms of data security.

Furthermore, if the public sector were to use only privacy-friendly services, this would be a positive signal for data protection, according to many respondents. However, the Bundeskartellamt's findings suggest that there could still be room for improvement here. Privacy-friendly messenger and video services do not seem to have prevailed over widely used services, both in terms of choice and paid use in the public sector. Industry representatives have provided numerous examples of how much effort and persuasion is needed to get privacy-friendly messenger and video services, which are less well-known than the established services, to be considered. This is especially true in areas where many consumers are to be reached, such as public broadcasting, but also in cities and municipalities, federal ministries or administrative units, as well as in the education sector.

As far as **data protection as a quality characteristic is concerned, it is not yet** apparent that many consumers base their choice of messenger and video service on its privacy-friendliness. If they do try, they have to cope with very unevenly distributed information - in favour of the services, to their detriment. Consumers would first have to find out what information is relevant in the first place, then search for it, gain a basic understanding and finally choose from several criteria

nor form an overall judgement and compare. In a **technically based industry,** insurmountable hurdles seem to present themselves: The technical criteria, procedures and practices that determine the data protection quality of a messenger and video service are complex and difficult for laypeople to comprehend. As a result, messenger and video services feel little pressure - at least away from the business customer segment - to enable consumers to make informed choices about data protection.
In the course of current developments, further challenges are emerging: the interoperability rules in the DMA will pose further challenges to data security and thus data protection. The services are technically set up differently. Many well-known services have been designed as closed systems. Users' data may thus be exposed to new risks. This circumstance requires high attention when interoperability is practised. However, at the same time, the information situation can become even more opaque for consumers.

*The **complexity of the necessary information can be** illustrated **by the example of encryption**, even if, for the sake of simplicity, deeper technical details and designations are not included. First of all, different **variants of encryption** must be distinguished. With transport encryption, the transport channel of a message is encrypted. However, it can be viewed both by users of the messenger and video service themselves and by the server operator. Unlike transport encryption, with end-to-end encryption ("E2E encryption") the message is sent encrypted across all transmission stations. Only the communication partners as end points of the communication can decrypt the data. Both variants can be used individually or in combination. The latter offers the highest level of security. **Various cryptographic methods are used** for encryption, such as symmetrical or asymmetrical encryption with public and private keys. In practice, end-to-end encryption is implemented using different technical standards, depending on which form of communication - text message, audio/video exchange - is used and which messaging and video system is used. In addition, there are **numerous technical limitations so** far that would also stand in the way of possible interoperability. On the one hand, this concerns the encryption of **text messages in groups (group chat)**, which becomes more and more complex with increasing group size. The solution in the form of the new standard Messaging Layer Security (MLS) is being tested in isolated cases. In addition, a new working group has been set up at the IETF to develop solutions for interoperable messaging and will also use the MLS standard for this purpose. It remains to be seen whether and to what extent and when there will be widespread implementation in the industry. End-to-end encryption is also currently subject to technical limitations in **videoconferencing and webinars.** In general, end-to-end encryption requires that participants are technically capable of providing and applying the necessary encryption functions. All participants must be on the same security level. Conversely, E2E encryption cannot be achieved as soon as one participant falls below the required security level.*

*This occurs, for example, when participants use a so-called **WebRTC client.** WebRTC is a protocol that is anchored directly in the browser and can only encrypt end-to-end between two end points. If there are more than two participants in a video conference, these are the end device of the user and the server of the service, which no longer meets the requirements of end-to-end encryption.*
*Even with certain **functions** that users like to use in videoconferences, end-to-end encryption cannot currently be technically connected: These functions include, for example, **dialling in from the public telephone network** or **the recording of meetings** by the service offering them. This is only possible if the service provider can access the data stream to include the audio call or record the data. The **connection of certain external devices** (e.g. room conferencing system devices based on the SIP protocol) is also not possible under end-to-end encryption, as this would require synchronisation of the different protocols. Leading services have explicitly pointed out just such limitations and others, such as the **use of "assistants".***
*Large video conferences for **webinars with several hundred participants** cannot currently be technically secured by end-to-end encryption. In this use case, it is necessary to check whether the service provider operates a video service location in Germany and whether this has been security-checked (for example, by a BSI C5 certificate). Transport encryption and the secure operation of the video service in Germany should be the criteria for this. Furthermore, care should be taken to ensure that the identity of the*
participants can be ascertained beyond doubt ("authentication"). End-to-end encryption ensures the integrity of the transmitted data. Without prior unambiguous authentication, it ensures the protection of the transmitted data, but does not ensure who can receive this data.

In the Bundeskartellamt's checklist, which could form the basis of an assessment of the data protection quality of messenger and video services, **encryption** is **only one of several criteria that** consumers would have to access. Against this background, it does not seem reasonable and purposeful to assign the responsibility for more competitive data protection to consumers alone, even if the information were to be extremely compressed and simplified for consumers.
Measures in favour of data protection quality must also include services. Measures that can strengthen data protection as a competitive parameter should therefore be placed alongside effective enforcement of the applicable law.

Evaluate data protection quality comparatively and transparently

In the Bundeskartellamt's current view, purely market-related measures may not be sufficient to help data protection out of its shadowy existence among the competition parameters and to attract the necessary attention. A transparent and comparative evaluation of the data protection quality of messenger and video services, e.g. with the aid of

of a rating procedure based on selected criteria of data protection and data security, could be helpful. **Such a procedure could** activate **both sides of the market** in terms of data protection. Initially, it is likely to trigger the greatest response on the side of the offering messenger and video services. It may be assumed that many messenger and video services would like to avoid a **publicly negative report card or a worse ranking than the most important competitor.** Data protection is not only "law" - in Germany and Europe in the form of the DSGVO - but has also become a sensitive topic that is followed closely by the (professional) public and also receives attention in the political environment. The constant confrontation with the practices of some leading industry representatives and public reflection on government initiative due to undesirable practices and developments have also contributed to this. However, consumers may also not want to be registered with a messenger and video service that **ranks last**. Perhaps one of their contacts would also prefer to use a messenger and video service that has a lower data protection risk than the previously chosen service. This also applies when acting as a proxy for consumers: A published rating opinion from a trusted authority can be the **credible information that professional "decision-makers" or contacts for the** public at authorities and companies need to decide on the GDPR compliance of a messenger and video service and thus its possible use in their own institution.

The Bundeskartellamt recommends following up on the present report:

- The **enforcement of consumer rights should be strengthened**. The digital economy constantly poses new challenges to consumers, especially due to its technical basis, which are becoming increasingly difficult to contain despite the commitment of all players. The Bundeskartellamt's competences and experience in law enforcement can make a meaningful contribution to overcoming and shaping these challenges.
- Efforts to educate consumers, especially in favour of the development of media literacy, should be intensified. All population groups should
  be integrated into a **communication strategy for data protection.** A corresponding nationwide campaign should therefore use both internet-based digital media and traditional media such as television.
- One conceivable signal would be if the **public sector** were to offer privacy-friendly messenger and video services more strongly. Contact persons and decision-makers need reliable information **on the GDPR compliance of messenger and video services** - especially those services that are not in the focus of public interest. Therefore, institutions, organisations and companies could offer the

Provide staff with appropriate **written information letters, brochures and handouts.**

- **Interoperability** should not only be **innovation-friendly**, but also **consumer-oriented.**
  be implemented. The already complex technical and legal interrelationships of data security and data protection are likely to be even less manageable under interoperability. In any plans and efforts to design interoperability, including its technical challenges, those responsible must not lose sight of the **requirements of a secure consumer product on behalf of the** users.

A. Introduction

Since time immemorial, it has been the will of man to exchange ideas with others, to connect and to record thoughts and ideas. Such a process of understanding[7] is also called communication. To do this, a sender must transmit signs of whatever kind to a receiver. This description of communication is very close to the definition of modern messaging. In general, it seems as if the exchange so intensively practised by consumers via text messages, telephony and video telephony, including the sending of photos and emojis, revives all the developmental stages of the history of communication, albeit in a modern guise.

At first, people communicated through pictures that were painted or carved on rock faces or stones.[8] Today, communication via pictorial signs is once again in vogue. With messaging, for example, emojis have found their way into communication. Unlike in the past, however, many consumers now use picture symbols to express feelings. Later, other forms of communication were added, first the actual writing and finally photography. For consumers, it now seems indispensable to take photos with their smartphones and send them directly to their contacts via their messenger and video services.

Today, messaging wraps these long-established modes of communication in a modern guise. Unlike in the past, consumers today can **individually use and combine** the various functions that messenger and video services enable. Furthermore, previously established forms of communication such as email, letter post or SMS are available as additional communication channels.

---

[7] Cf. *The Lord Mayor of the Federal City of Bonn*, "What are you trying to tell me?" The History of Communication, available at: https://www.bonn.de/medien-global/amt-41/stadtarchiv/ Ausstellung_Geschichte_der_Kommunikation.pdf.

[8] Pictographic writing goes back primarily to the Sumerians in the area of present-day Iraq and the Egyptians, who developed a complex pictographic script in the form of hieroglyphs around 3000 BC. See, for example, *Planet Wissen*, available at: https://www.planet-wissen.de/gesellschaft/lernen/erfindung_der_schrift/index.html# Hieroglyphics, see *Wikipedia*, available at: https://de.wikipedia.org/ wiki/Geschichte_der_Schrift, see *ARD alpha, available* at: https://www.br.de/wissen/schrift- ursprung-keilschrift-mesopotamien-100.html, see Viaprinto, available at: https://www.viaprinto. de/blog/2016/06/die-geschichte-der-schrift/.

The **desire for individuality or a customised solution** for one's own needs is reflected in a great **variety of business models and applications in** messenger and video services. As the Bundeskartellamt has already pointed out in the interim report on this sector enquiry, the functions, the business models and the economic significance of messenger and video services are very diverse. In addition to the leading services popular with consumers, there is a wide range of industry participants, ranging from international, group-operated services with many millions of users, high revenues and their own digital ecosystems[9] with strong positions in neighbouring markets, to national services or services focused on German-speaking regions or services with a special business focus, to open source services and free applications without the intention of making a profit.

One concern of this sector enquiry was initially to reveal this diversity. There are several reasons for this.

The attention of supervisory authorities and data protectors often rests on a certain business model of leading messenger services, within the framework of which consumers' data is collected and utilised via a free offer. However, apart from these popular services, a differentiated industry has developed with considerable turnover and user figures, the composition of which is still unknown to large parts of the public. It was questionable whether and to what extent possible, with the leading

---

[9] The term "digital ecosystem" refers to a bundle of a multitude of services of a group with interactions among each other, cf. *Bundeskartellamt, Stellungnahme zur* öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25 April 2022, available at: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf as well as *Bundeskartellamt*, The Evolving Concept of Market Power in the Digital Economy - Note by Germany, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/OECD_2022_Competition_Committee_Concept_Market_Power_Digital_Economy.pdf?_blob=publicationFile&v=2. See also e.g. *Fletcher,* Digital competition policy: Are ecosystems different?, Note for the OECD Hearing on Competition Economics of Digital Ecosystems, available at: https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf. In information technology, the term ecosystem is used to describe a software and hardware architecture, each of which is based on its own devices, systems and access requirements and thus presupposes and generates corresponding accessories, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/%C3%96kosystem.

business model related **legal violations and also other consumer law failures** have become widespread in the industry. This concerns, for example, the disclosure of contact data, which is held up to the leading services as a violation of data protection law. It also concerns security failures, for example in encryption. If users are not adequately informed about security-relevant aspects of a messenger or video service, they could be unlawfully misled. Sector enquiries are the appropriate instrument here. They are not directed at specific companies, but take a look at an industry as a whole. Furthermore, demands for interoperability had repeatedly arisen in the political arena.[10] In the meantime, these **political demands have been** reflected not only in the coalition agreement, but also in the interoperability regime of the Digital Markets Act[11] . In the interim report, the Bundeskartellamt already explained and proved with the results of its investigations that the analysis of the interrelationships between competition, data protection and innovation is multi-layered and complex. In this final report, the focus is now on the **concrete implementation of** an interoperability project for which it is hardly possible to estimate how it will actually be used. A challenge is not only the diversity of the technical architecture of messenger and video services and the individual adaptations of international standards. Especially when the personal data of users is passed through further hands in an international business, new solutions must be sought without losing sight of the overall economic costs.

---

10 Cf. *Verbraucherschutzministerkonferenz*, Ergebnisprotokoll der 15. Verbraucherschutzminister-konferenz am 24. Mai 2019, TOP 12, Nr. 2, available at: https://www.verbraucherschutz ministerkonferenz.de/documents/ergebnisprotokoll-der-15-vsmk-am-24052019-in-mainz_rlp-extern_ 1559902425.pdf as well as Handelsblatt of 15.09.2019, Interview with *Katarina Barley*, Die Datenschutz- Grundverordnung ist ein scharfes Schwert, available at: https://www.handelsblatt.com/politik/ international/europawahl/katarina-barley-im-interview-die-datenschutz-grundverordnung-ist-ein- scharfes-schwert/24339900.html and *Golem.de*, Politicians demand interoperability, 2019, available at: https://www.golem.de/news/messenger-was-bringt-eine-fusion-von-facebook-whatsapp-und- instagram-1901-139014-2.html.

11 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14.09.2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265/1 of 12.10.2022 (Digital Markets Act) - DMA, available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925&from=EN .

After all, the heterogeneity of the sector is also a reflection of consumer wishes, which are quite diverse and different. The same applies to the conditions under which consumers make decisions. This does not only concern a distinction between business and private plans, to which the Bundeskartellamt refers in its investigation results when necessary. Rather, a more **differentiated consumer model** has recently been discussed in the expert public, which describes consumers as responsible, vulnerable or trusting .[219][220] In this respect, there seems to be a broad consensus that differences between consumers in terms of their perception, emotion and motivation must be taken into account.[221] This is not only true when it comes to their need for protection, which is the focus of the recommendations for action in this sector inquiry report. A realistic consumer model is also important so that appropriately adapted measures are taken to motivate consumers to advance data protection as a competitive parameter and to better protect their data.

The demands on the recommendations for action are therefore high. Not only the diversity of the industry, but also the political stipulations on interoperability as well as the wishes and behaviour of consumers must be taken into account and integrated as best as possible when formulating recommendations for action for a higher level of data protection. Measures would thus be necessary to **motivate both sides of the market to** give more priority to data protection in the competitive process. This does not only refer to stopping the violations of consumer law which are examined in this report. In particular, it is about better information for consumers and, in the course of this, more committed practical implementation of competitive data protection. It is also a question of how the public sector is committed to a higher level of data protection, even outside of legal proceedings conducted by the competent authorities. In the case of interoperability projects and the associated desire for increased switching activities by consumers, it must also be taken into account that, from their perspective, there is likely to be a lack of transparency and comparability on data protection quality already in bilateral exchanges via messenger and video services.

Following this introduction, the **procedure of** the consumer sector enquiry will be briefly explained (see chapter B.).

This is followed by a brief description of the **industry in** its diversity and with its main characteristics (see chapter C.) as well as the economic and competitive environment.

It then outlines how **key security criteria and the way data** is **processed** can affect the privacy-friendliness of a service and the industry's practical position on this (see Chapter D.). This is followed by an assessment of the results. It

an orientation for the evaluation is first introduced with the perspective of the consumers and the state of the art, before conclusions are drawn from the results of the investigation on the safety criteria as to what would be desirable. This is followed by a **legal classification. It** is questioned how the common practice of many well-known messenger and video services to upload and synchronise the contact directory of users is to be evaluated from a data protection perspective. It will also be examined to what extent messenger and video services comply with data protection regulations when transferring data to third countries and storing it on servers in third countries, according to the results of the investigation. Finally, the chapter looks at whether the services' information behaviour on end-to-end encryption can trigger violations of transparency obligations under fairness law. The chapter ends with a conclusion on whether and to what extent consumers can best deal with the current situation.

This is followed by discussions on **data portability**, which was introduced in Art. 20 GDPR and was generally linked to the hope of facilitating consumer switching plans and could thus represent a transition to interoperability (Chapter E.). Here, too, the theoretical considerations are followed by the results of investigations, which can be interpreted as an indicator of consumers' switching behaviour.

After that, we move on to the next focus of this report, the examination of the guiding question of whether and to what extent **interoperability** could lead to **a higher level of data protection** (Chapter F.).

First of all, a conceptual, legal and scientific classification is provided (see F.I). Unlike in consumer law regulations, under competition and telecommunications law, the authorities can - under high preconditions and in a defined procedure - issue an interoperability obligation. Meanwhile, the legal framework for messenger and video services is supplemented by the Digital Markets Act. This came into force in November 2022 and has led to a concretisation of the legal environment for messenger and video services in terms of interoperability. Namely, designated services, so-called "gatekeepers" in the sense of the DMA, are imposed regulations on the interoperability of certain basic functions. The complexity of the guiding question is also suggested by the numerous scientific studies, of which a brief overview is then given. This is followed by a brief description of the possibilities for technical implementation and design. The differences lie not only in the depth of technical intervention and the effort required. The measures also differ in terms of scope and the necessary degree of willingness to reach a consensus on the part of those involved. Finally, the behaviour of consumers is essential for the future market development of messenger and video services, including interoperability (see F.II).

The results of the investigation on interoperability are then presented in detail (see F.III). In addition to what was said in the interim report, the industry's position on functional and technical design and standardisation is included (see F.III.3.b and c). At the end of the chapter, initial conclusions can be drawn (see F.IV). Any regulatory or legislative measures aimed at eliminating problematic situations must be designed in such a way that opportunities **for further market development are** also **preserved**. In this context, it is also interesting to see how the opinions expressed in advance by the messenger and video services and the current legislative plans compare.
What scenarios are conceivable for the further development of the industry with regard to interoperability in view of consumer behaviour and how should this be dealt with?

Against this background, Chapter G. presents **concrete approaches on** how the level of data protection in messenger and video services could be improved. In its questionnaire, the Bundeskartellamt had asked the services to comment on and evaluate various proposed measures (see G.I). Against the background of the results of this investigation, the Bundeskartellamt has taken up some aspects which could give greater weight to data protection in competitive processes (see G.II). To this end, improvements for data protection-friendly messenger and video services are first presented, which can be implemented promptly and with comparatively little effort. Subsequently, the role of targeted information for consumers making enquiries will be discussed. Will the level of data protection improve in this way - driven by the market - under the given framework conditions? The chapter concludes with comments on a comparative and transparent evaluation of data protection quality - on rating - an instrument that seems suitable to motivate both sides of the market to understand data protection as a competitive parameter and to actively take it into account in selection processes (see G.III).
The report concludes with **recommendations for action to improve the level of data protection** in messenger and video services (see H.). Due to the diversity of the industry and the many sustainable business models and free applications in addition to the well-known market leaders, the Bundeskartellamt does not only want to contribute to more transparency with this report. Rather, it is intended to provide macroeconomically beneficial, concrete indications for improvements in consumer protection. All areas and stakeholders are to be included in such a data protection strategy, both the system of consumer law enforcement (on this under H.I) and the consumers (on this under H.II) as well as the messengers and video services themselves (on this under H.III). Finally, characteristics of an innovation-friendly and consumer-oriented interoperability concept are presented that

can have a positive effect for the benefit of all the addressees mentioned and promote data security and data protection (see H.IV).

B. Course of proceedings

I. Consumer Law Sector Inquiry

In November 2020, the Bundeskartellamt launched a consumer sector enquiry into the "Messenger services" initiated under Section 32e (5) ARC.[12]

In the run-up to the investigation and during the investigation period, the Bundeskartellamt established and maintained contact with other authorities and institutions which are involved in the consumer protection issue of messenger and video services or are themselves concerned with it. These include the Federal Office for Information Security (BSI, see Chapter II), the Federal Commissioner for Data Protection and Freedom of Information (BfDI), the Federal Network Agency (BNetzA), Stiftung Warentest and the North Rhine-Westphalia Consumer Advice Centre (VZ NRW).

Furthermore, the Bundeskartellamt held talks with market participants and experts in order to specify the topics of the investigation and to prepare the survey.

On 31 May 2021, the Bundeskartellamt sent extensive questionnaires[13] to the operators of 53 messenger and video services in Germany and abroad. Two respondents were subsequently removed from the list of addressees. The response rate to the questionnaires was

28 June 2021. Various extensions have been granted until 27 July 2021. 44 messenger and video services (86 percent of respondents) answered the questionnaire.[14] The information provided by these services forms the basis for the results of the investigation presented below.

The Bundeskartellamt presented the interim report on the sector enquiry on 4 November 2021.[15] The results of the interim report have been incorporated into the final report. The comments on the sector (Chapter C.) were taken from the interim report, partly with minor changes,

---

12 Cf. *Bundeskartellamt*, press release of 12.11.2020, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_SU_Messenger_Services.html?nn=3591568.

13 The questionnaire sent to the services surveyed is available here: www.bundeskartellamt.de/messenger.html.

14 See list of included services in the appendix.

15 Cf. *Bundeskartellamt*, press release dated 04.11.2021, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/04_11_2021_SU_Messenger_Services_Interim_Report.html?nn=9624654.

on data portability (Chapter E.) as well as in parts individual sections of Chapter F. on the results of investigations on interoperability (see F.III.4 and F.III.5).

II. Cooperation with the BSI

In the context of the sector enquiry into messenger and video services, the Bundeskartellamt has exchanged views in particular with the Federal Office for Information Security (BSI). The BSI is the federal government's cyber security authority. The BSI's remit is defined by the Act on the Federal Office for Information Security[16] . The BSI investigates and evaluates existing security risks and assesses the impact of new developments.[17]

On 22 January 2021, the Bundeskartellamt and the BSI signed a Memorandum of Understanding with the aim of pooling their respective competences and expertise, particularly in digital consumer protection.[18] In connection with the present sector enquiry, the BSI examined the planned topics of the enquiry from a technical point of view and advised the Bundeskartellamt in particular on the formulation of questions on technical aspects of data security within the framework of the questionnaire and provided a glossary of cryptographic terms. At the same time as the interim report, the BSI issued its own publication on the security requirements and characteristics of messenger services from the consumer's point of view. The BSI publication

describes the basic functionalities of messenger systems and focuses in particular on the topics of encryption, meta-data/data protection and interoperability.

---

16 Act on the Federal Office for Information Security of 14.08.2009 (BGBl. I p. 2821), last amended by Art. 12 Act of 23.06.2021 (BGBl. I p. 1982) - BSIG.

17 Among other things, the BSI has developed a comprehensive range of information for consumers and companies on digital security issues. The BSI is also concerned with questions of consumer protection in the digital sector. According to Section 7 BSIG, the BSI can issue warnings if there are security vulnerabilities in information technology products and services. According to § 7a BSIG, information technology products and systems can be investigated by the BSI, cf. *BSI*, available at: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html.

18 Cf. *Bundeskartellamt*, press release of 22.01.2021, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/22_01_2021_Zusammenarbeit_BSI_BKartA.html.

C. Industry overview of messenger and video services

Messenger and video services offer a range of basic communication services. Consumers can not only exchange text messages bilaterally (1:1) but also in groups, make phone calls (via video) and send photos, videos, voice messages and other files. In this sector enquiry, the Bundeskartellamt does not only refer to exchanges via text messages. For the purpose of this investigation it has decided on a broad definition of messenger and video services. Thus, the term messenger service is used as a collective term for open and closed messaging systems, messenger clients and multi-messengers which offer messaging functions and/or video telephony (individually and/or in groups, such as in video conferences, online meetings, webinars, etc.). The same applies to the term video service, under which all systems and applications of video telephony (individually and/or in groups, such as in video conferences, online meetings, webinars, etc.) and, where applicable, messaging functions (individually and/or in groups) are covered.

The reasons for this lie in the development of the industry, where many individual business models and applications have emerged and are constantly being developed. More and more messenger and video services offer similar functions, albeit with different focuses. Even the boundaries with social networks and software providers appear fluid. Finally, consumer law failures can affect all messenger and video services and are not limited to specific functions.

In the following, we will first look at how communication via the internet ("messaging") works, what consumers need for this and what functions messenger and video services offer consumers (see I.). Subsequently, the relationship between messenger and video services and other forms of communication will be briefly explained (see II.). Since technical development plays a major role in the topics under investigation, it is also explained how open standards are developed in the industry (see III.). The chapter concludes with initial findings on industry participants, financing, usage figures and the competitive situation (see IV.).

I. Functionality and functions

The origins of messaging lie in chat, i.e. electronic communication by means of written text in real time, mostly via the internet.[19] Today's range of messenger and

[19] Cf. *Wikipedia,* available at: https://de.wikipedia.org/wiki/Chat.

video services is based on the same technology. Users must first select and use a user software (client). A client is a programme or application that runs on a user's terminal device and is accessed via a server.
(central computer). Many messenger apps can be used equally on mobile and stationary end devices, such as smartphones or desktop computers, and in some cases also via the internet browser.
As a rule - if a server is used - messages can also be sent when the conversation partner is not currently online; the message is then temporarily stored by the server and later delivered to the recipient when he or she is available again.
Many messenger and video services additionally support **group chats, telephony, video telephony and the transfer of files as well as audio and video streams**. Which functions are offered in detail can vary depending on the messenger and video service. The range of functions is significantly influenced by the so-called protocol used by a messenger service. The protocol can also be described as the technical language of a messaging system.
Among messenger and video services, **video conferencing providers** are those services that offer video conferencing as a business focus. The boundaries to consumer-oriented services with a focus on messaging are fluid. In most cases, video conferencing providers also offer text messaging in addition to their core video telephony/conferencing service, albeit possibly only within certain apps for business customers.[20]
During the **Covid 19 pandemic, the** number of users of video services increased sharply. This effect need not be short-term. In the wake of the pandemic, work organisation and trends in the professional world have changed, e.g. the increased establishment of home offices. The positive effects have left a lasting impression. For this reason, too, it can be expected that digital communication methods will continue to be of great interest in the future. Furthermore, the sometimes fluid demarcation between services or functionalities used primarily for private or business purposes is not relevant for the sector enquiry. Questions of data protection law arise independently of this. At the beginning of the Corona pandemic, when many consumers were increasingly communicating via videoconferencing, the Bundeskartellamt was

[20] Cf. for other messenger services with a focus on video conferencing, e.g. *Gesellschaft für Datenschutz und Datensicherheit* (2020): GDD-Praxishilfe DS-GVO XVI - Videokonferenzen und Datenschutz, Annex 1, available at: https://www.gdd.de/aktuelles/startseite/neue-praxishilfe- videokonferenzen-und-datenschutz-erschienen.

received enquiries from various sides concerning data protection issues with video conferencing providers.

II. Relationship to other means of communication

The means of communication considered here, messaging and internet telephony, are used via the Internet, and thus "over-the-top" (OTT).[21] OTT services can in turn be divided into different categories. According to the categorisation of the Body of European Regulators for Electronic Communications (BEREC), messenger services correspond to the category OTT-1 services.[22] OTT-1 services can enable voice transmissions via the internet (internet telephony) and thus compete with classic telephony services.[23] However, they are independent of fixed network or mobile phone connections and therefore do not allow connection to classic telephony services with so-called E.164 numbers.
Even though the functions are similar, voice telephony and SMS can be distinguished, at least technically, from messaging and internet telephony. **Voice telephony** refers to voice communication via a technical device. The transmission takes place either through analogue or digital telephone services, such as a radio network or a packet-switched data network.[24] **Short Message Service** (SMS) is a telecommunication service through which

---

21 Cf. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung, available at: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile&v=6, p. 9 f.

22 Cf. *BEREC* (2016), Report on OTT Services, BoR (16), 35, p. 15 - 17. BEREC forms three categories. OTT-0 are services that can establish connections to classic telephone services via mobile telephone numbers. Messenger services belong to the so-called OTT-1 services. Content-based applications that are not primarily used for communication are referred to as OTT-2 services.

23 *Body of European Regulators for Electronic Communications (BEREC),* Report on OTT services, January 2016, p. 14 f., available at: https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf.

24 Cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Telefonie.

text messages, usually called "short messages" or "SMS", can be transmitted.[25] SMS is based on GSM technology.[26]

Unlike number-based voice telephony and SMS, **e-mail** (electronic mail for "electronic mail") is web-based just like messenger services and is one of the so-called OTT-1 services. E-mails are letter-like messages transmitted via the internet. Both text messages and digital documents can be sent to their recipients anywhere in the world in a matter of seconds. E-mail is an open standard that has been around since 1968. It is based on SMTP[27] -, IMAP[28] - and POP[29]- protocols.[30] The various e-mail servers are linked via the e-mail protocol so that messages can be sent between different providers.

---

[25] SMS was first developed for GSM mobile telephony and is also available in various countries as fixed network SMS.

[26] GSM (Global System for Mobile Communications) is a mobile radio standard for fully digital mobile radio networks, which is mainly used for telephony, but also for circuit-switched and packet-switched data transmission as well as short messages. It is the first standard of the so-called second generation ("2G") as successor to the analogue systems of the first generation, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications.

[27] SMTP ("Simple Mail Transfer Protocol") is an Internet protocol that is used to exchange e-mails in computer networks. It is primarily used for sending and forwarding e-mails, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

[28] IMAP ("Internet Message Access Protocol") is a network protocol that provides a network file system for e-mails. Via IMAP, the complete content of a user's email account is always synchronised with the mail programme on his or her computer or smartphone. All folders are synchronised so that the user can use the identical inbox from all devices, see *Wikipedia,* available at: https://de.wikipedia.org/wiki/Internet_Message_Access_Protocol.

[29] POP ("Post Office Protocol") is a transmission protocol via which a client can send e-mails from a e- mail server can fetch. Using the POP3 version ("Post Office Protocol Version 3"), only the e-mails from the folder of the inbox are downloaded from the server. The POP3 procedure is only used for simple downloading of the inbox. There is no synchronisation between the end device and the email account, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Post_Office_Protocol.

[30] Cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/E-Mail.

can be created.[31] Users can open an account with any provider. Data protection aspects have been and are still being discussed in expert circles with regard to e-mail to the same extent as with messenger services.

BEREC has also included **social networks in the** OTT categories. Social networks, just like streaming platforms or search engines, are categorised as so-called OTT-2 or "content-based" OTT services.

In competition law proceedings, the European Commission and the Bundeskartellamt have worked out the differences between messenger services and social networks. The Bundeskartellamt found that in the case of messenger services there was a "[bilateral] communication or

Group communication within smaller groups"[32] takes place and the information exchanged is typically of limited temporal relevance. The definition of the European Commission includes very similar providers with the term "consumer communications app", but at least considers an inclusion of e-mail or SMS.[33] However, there are clearly different functionalities between social networks and consumer communications apps.[34] In communication networks, users who already know each other typically communicate with each other, whereas in social networks, indirect communication with people who are not yet known is also possible, or often even desired.[35]

For the definition of the industry under consideration in a (consumer law) sector enquiry, a market definition according to antitrust standards is not necessary. The results of the investigation give the impression that there are business models, especially in the US and in Asia, in which **content-based services and functions of typical messenger and video services with a focus on message exchange are mixed** and that this development is continuing. Here, in the course of further development

---

31 Cf. *Kuketz*, Die verrückte Welt der Messenger - Teil 1, available at: https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/.

32 *Bundeskartellamt*, Decision of 06.02.2019, B6-22/16, para. 290 - *Facebook*.

33 *European Commission*, Decision of 03.10.2014, COMP/M 7217, para. 20 et seq. - Facebook/ WhatsApp.

34 *European Commission*, Decision of 03.10.2014, COMP/M 7217, para 61 - Facebook/ WhatsApp.

35 *Bundeskartellamt*, B6-113/15, Working Paper - Market Power of Platforms and Networks, June 2016, S. 101.

changes are taking place anyway. **Virtual reality**[36] **and augmented reality**[37] may also become standard features of messenger and video services and social networks. With these new functions, users can use aids such as VR glasses to enter artificially created worlds in real time - while they are in their normal environment - or call up relevant additional information with the help of a computer. In contrast to virtual reality, augmented reality retains the real environment and is merely supplemented by individual virtual information.

III. Standardisation procedure

Messenger and video services function on the basis of (communication) protocols[38] and other technical components. In accordance with the importance of technical functionalities, the industry has a certain technical self-organisation through **internationally recognised standardisation organisations**. Foremost among these is the **Internet Engineering Task Force (IETF)**, whose focus is on the standardisation of the communication protocols used on the Internet. Standardisation processes are also important for the messenger and Internet industry.

---

36 "Virtual reality" (VR) refers to a digital image of reality created on a computer. VR glasses allow users to immerse themselves in a new, artificially created world that looks deceptively real. For example, they can swim with whales in underwater worlds, explore a shipwreck or walk through their new house before it is built, cf. *Deutsche Telekom*: Einfach erklärt - Augmented und virtuelle Realität, available at: https://www.telekom.com/ de/konzern/details/virtuelle-realitaet-486114, or *Wikipedia,* available at: https://de.wikipedia.org/wiki/Virtuelle_Realit%C3%A4t.

37 Augmented reality" (AR), on the other hand, is the interaction of digital and analogue life. This can work via the smartphone camera or, as is usually the case, via a pair of glasses, whereby the user is not completely cut off from his or her normal environment as is the case with VR glasses. Rather, additional information about his or her environment is displayed in the glasses. For example, a warehouse worker can be shown on which shelf the spare part he is looking for can be found, or the mechanic can be given useful information about the technical component she is to repair, cf. *Deutsche Telekom*: Einfach erklärt - Augmented und virtuelle Realität, available at: https://www.telekom.com/de/konzern/details/virtuelle-realitaet-486114.

38 Communication protocols define the rules for data transmission between the end points of communication. They are virtually the language of a messaging system by means of which the various units of the technical system communicate with each other.

video services if interoperability were implemented via standards. Accordingly, the Bundeskartellamt surveyed the industry on aspects of standardisation. In turn, the companies surveyed frequently referred to standardisation procedures with their advantages and disadvantages in their answers. Among the international institutions relevant to the industry in standardisation processes, the IETF was mentioned most frequently in the sector enquiry. It is an open, international voluntary association of network engineers, manufacturers, network operators, researchers and users that is concerned with the technical development of the internet in order to improve its functioning.[39]

The W3C was also referred to several times by the interviewed companies. The **World Wide Web Consortium (W3C)** is a member organisation for the standardisation of techniques in the World Wide Web.[40] Some respondents pointed out that the W3C was instrumental in developing the **WebRTC standard.** This is an open standard that defines a collection of communication protocols and application programming interfaces (API) that enable real-time communication over computer-to-computer connections. Applications such as video conferencing,

File transfers or data transfers, chat and screen sharing can function in this way.[41]

In addition, there are other standardisation bodies, such as the XSF (XMPP Standards Foundation) as a non-profit foundation, which specifies and further develops the XMPP protocol.

The **process at the IETF** starts with proposals from industry, which are discussed in an initial meeting (so-called Birds of a Feather session, BoFs) during one of the three annual IETF meetings. If the topic is pursued further, a working group is formed. Once consensus on a draft paper is reached at some point, a draft slowly approaches a so-called "draft". This is an early version of a possible standard that can and should now be discussed outside the actual working group. This can happen in events at IETF meetings, other industry meetings or via publications for the Internet community.[42]

---

39 Cf. *IETF*, available at: https://www.ietf.org/about/, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Internet_Engineering_Task_Force.

40 Cf. *W3C*, available at: https://www.w3.org/, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/World_Wide_Web_Consortium and other publicly available sources.

41 Cf. *Wikipedia*, available at: https://en.wikipedia.org/wiki/WebRTC.

42 Cf. *NETPLANET*, https://www.netplanet.org/organisation/standardisierung.shtml.

Drafts and later also the finished standard are published as **RFC (Request for Comments).** The RFC documents form a clear basis for standardisation processes and the development of network technologies on the Internet. The publication of RFCs is managed by the so-called RFC Editor. This is an independent body funded by the Internet Society .[43]

The extent to which working groups of the IETF are influenced by the interests of large companies is a recurring topic of discussion among experts. On the one hand, it is said that the openness of the standardisation work could become a problem if large companies send numerous employed developers to influence the decision-making in a working group.[44] The aim could be to spread their own software patents over the respective standard (so-called **standard essential patents**, SEP).[45] On the other hand, there are reports,

z. e.g. about the failure of China to push through a new internet protocol in the IETF because it was lacking in the

"basic principles of the internet such as anonymity and equal status of data traffic"[46] shakes.

In principle, standardisation organisations adopt internal rules for dealing with proprietary technologies. This also applies to the IETF. Even if these rules are designed differently, they usually share two elements. On the one hand, participants in the working groups are requested to disclose standard-essential patents (SEPs). However, neither members nor the organisation itself will search for relevant patents or check for disclosed patents,

---

43 The Internet Society (ISOC; German Internet-Verband) was founded in 1992 at the INET conference in Kōbe (Japan) and is responsible as a non-governmental organisation for the maintenance and further development of the Internet infrastructure, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Internet_Society.

44 Cf. in this context the report on the search for uniform spam measures, during which Microsoft wanted to position its own standard as the basis of the open standard, see *Netplanet*, available at: https://www.netplanet.org/ organisation/standardisation.shtml.

45 See for a detailed discussion of the topic e.g. *Max Planck Institute for Innovation and Competition* (2015): Standard Essential Patents: The Role of Standardisation Organisations, Research Report 2015, available at: https://www.mpg.de/9853703/jb_20151.

46 *Wirtschaftswoche* of 4 May 2020: Hum for the Internet, available at: https://www.wiwo.de/technologie/digitale-welt/web-standards-brummen-fuers-internet/25779644.html.

to what extent they are essential for the standard.[47] Secondly, the declaration of SEPs is linked to the patent holder's self-commitment to grant licences on fair, reasonable and non-discriminatory terms (so-called FRAND principle, fair, reasonable and non-discriminatory).[48]

This process of developing open standards via standardisation organisations also touches on the issues of the sector enquiry. In the meantime, the IETF has completed work on a standard that should make more comprehensive encryption possible for exchanges in groups. Specifically, it is about a security layer for end-to-end encryption of messages in small and large groups (so-called **Messaging Layer Security**[49] **, MLS**). According to public information, the BoFs took place in London in February 2018. The founding members were then Mozilla, Facebook, Wire, Google, Twitter, University of Oxford and the French National Research Institute for Informatics and Automation (INRIA). In the first quarter of 2023, a new MIMI working group met for the first time at the IETF, which will work on open solutions for interoperable messaging.[50]

IV. Investigation results

The industry of messenger and video services is diverse, so that possible measures and legal regulations will have different effects on the companies concerned. In this respect, knowledge about the provider side is essential in order to be able to correctly interpret the results of the investigation as well as to later evaluate possible consumer law violations and formulate targeted recommendations for action. Furthermore, a broader presentation enables

---

47 Cf. *Max Planck Institute for Innovation and Competition* (2015): Standard Essential Patents: The Role of Standardisation Organisations, Research Report 2015, available at: https://www.mpg.de/ 9853703/jb_20151.

48 Cf. *Max Planck Institute for Innovation and Competition* (2015): Standard Essential Patents: The Role of Standardisation Organisations, Research Report 2015, available at: https://www.mpg.de/ 9853703/jb_20151 and *IETF* (2017): At Long Last, A Revised Patent Policy for *IETF*: What's Behind BCP79bis?, available at: https://www.ietf.org/blog/whats-behind-bcp79bis/ or: https://www.ietf.org/standards/ipr/.

49 Cf. https://datatracker.ietf.org/wg/mls/about/, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Messaging_Layer_Security.

50 See *IETF*, Messaging Layer Security: Secure and Usable End-to-End Encryption, available at: https://www.ietf.org/blog/mls-secure-and-usable-end-to-end-encryption/ and golem, IETF standardises protocol for secure group chats, available at: https://www.golem.de/news/messaging-layer- security-ietf-standardisiert-protocol-fuer-sichere-gruppenchats-2303-173089.html.

the industry provides consumers with good orientation and information about possible alternatives beyond the generally known, large services.

1. Industry participants, functions and business models

From the preliminary talks on the sector enquiry, the Bundeskartellamt had already gained the impression that the sector is extremely heterogeneous. The investigations confirm this and paint a clear picture of the diversity of market participants. Behind messaging and video services is a large industry with a wide variety of business areas and a broad field of non-commercial applications.

In terms of **geographic reach,** the scale could not be larger. For one thing, messaging and videoconferencing is home to many **globally active, diversified technology groups and globally active digital corporations** that are already successful and hold strong positions in other markets.
These are, for example, Cisco as a manufacturer of network technology and end devices with the video conferencing company Webex, Google as a manufacturer of operating systems and search engine with Google Meet, social media platform operator Meta (formerly Facebook) with WhatsApp and Facebook Messenger, operating system and software manufacturer Microsoft with Microsoft Teams and Skype and also companies such as the Japanese Line Corporation, which belongs to the South Korean Naver Corporation. Naver operates a search engine, which is in high demand in some regions, an email system and offers digital information. These services are thus a business that takes place worldwide. On the other hand, regional or national services, niche providers such as Univado (e-learning) or messenger and video services that are less known to the general public, such as Ginlo, are also active in this industry.
There is also an **open source area, which** includes services whose business model is interoperability, as well as the large world of free messaging systems, i.e. those that are independent of central providers. The latter includes the long-standing protocol XMPP with a fixed community as well as matrixes and systems based on the IMAP and SMTP protocols used for e-mail. These services are basically free of charge for consumers.
The heterogeneity is also reflected in the technical structure. According to the **technical integration/depth, a** distinction must be made between systems and clients. A messaging or video **system** includes all the elements needed for messaging or video conferencing. It consists of the communication protocol, server software, hardware and the user software (app, client). The so-called **clients or apps are** a programme that is executed on the end device of a network and communicates with a server (central computer). Among the clients, the so-called **multi (protocol) messengers** correspond to a software that can use a multitude of

communication protocols and enables users to operate different messenger systems via one software interface. However, cross-system message exchange is not possible. Also, multi-messengers often do not fully support the functional possibilities offered by the respective protocol.

According to the **independence from a central service provider,** so-called closed systems can be distinguished from free systems.

In **closed systems,** all elements and properties of the system, especially the client and the servers through which data is exchanged and stored, are specified by the service provider.

Free messenger systems function similarly to e-mail services. They are technically based on a standard protocol (usually XMPP or Matrix) so that users can exchange messages across different messenger clients. Thus, conversation partners do not have to have the same app installed in order to communicate with each other. There is no one all-determining service provider. They are federated systems that have decentralised server structures. This means that there is generally no central data storage. Users choose a server provider that best implements their preferences. They can further choose between different clients for different operating systems and opt for the one that best meets their requirements.

The best-known and most widespread free messaging systems are XMPP, Matrix and systems that use the protocols used for e-mail. In addition, there are other free messenger systems such as Goldbug, Mattermost and many more.

XMPP (Jabber) is a federated, decentralised system for instant messaging that can be used independently of a central service provider. The extensible basic protocol is standardised by the Internet Engineering Task Force (IETF) and defines how clients and servers as well as servers can exchange data packets with each other. What information is actually transmitted in these packets is defined via extensions. These extensions, called XEPs (XMPP Extension Protocol), are defined by the XMPP Standards Foundation (XSF) - the standardisation body.

standardised. Extensions exist for all possible purposes, such as OMEMO for the End-to-end encryption.[51] To be able to chat on the basis of XMPP, a user account must exist or be created on any server. Similar to e-mail, users are not

[51] Cf. *Golem,* OMEMO: Finally encrypted chatting on many devices, 12 October 2016, available at: https://www.golem.de/news/omemo-endlich-auf-vielen-geraeten-verschluesselt-chatten-1610-123621.html.

Users identified via username@server. They can operate their own server. However, this requires a certain technical understanding and commitment. Therefore, there are many different public providers on whose server the administration of accounts, address books and chat histories of the users can then take place for several devices if necessary. With XMPP, there are many hidden user groups with an estimated several million users. These include, for example, operators of online games. According to the community, XMPP is used by NATO and is also being tested by the German Federal Police.[52] WhatsApp also originally developed its closed protocol on the basis of XMPP.

Among the XMPP clients, the Federal Cartel Office received responses from Conversations, Quicksy and Yaxim (all for Android), for Apple's iOS from Monal and for Linux from Gajim, Dino and Profanity. **Matrix** has been under development since 2014. The system is not currently defined as an internet standard by the IETF. Unlike XMPP, Matrix does not consist of different or extendable modules. When new or changed requirements arise, the protocol is modified or supplemented as a unit. Matrix also allows users to communicate with each other in real time, regardless of the clients they use. In the philosophy of Matrix, basically every chat is a room. The focus is on the fail-safe nature of chat rooms. Chat rooms are synchronised among all participating servers of the participants (all messages of the room are stored on each participating server). This means that in the event of a server failure, all participants from other servers can continue to use the chat room as normal.[53]

For Matrix, the probably best-known client Element was included in the study. According to Element, Matrix is used at many German universities and BWI[54] - the IT system house of the

---

52 Cf. for a detailed presentation *Initiative freie Messenger*, available at: https://www.freie-messenger.de/introduction/.

53 Cf. *Initiative freie Messenger,* Matrix, available at: https://www.freie-messenger.de/sys_matrix/.

54 See *BWI*, Open-Source: "Matrix" ist einheitlicher Messenger-Standard für die Bundeswehr, available at: https://www.bwi.de/news-blog/news/artikel/open-source-matrix-ist-einheitlicher-messenger-standard-fuer-die-bundeswehr The abbreviation used to stand for Bundes-Wehr und Industrie, but is no longer used in this way, see *BWI*, available at: https://www.bwi.de/das-macht-die-bwi.

Bundeswehr - used. Gematik[55] has selected the Matrix protocol as the standard for messaging in the health sector.[56]

E-mail as a messaging system is characterised by great accessibility. Every user can communicate with any e-mail address without the recipient needing the same or a special messenger programme. The messenger client functions here like a classic messenger, but uses the proven e-mail infrastructure, including the standardised and open protocols IMAP[57] and SMTP[58] . [59] The e-mail system is in the Sector enquiry represented by the client "Delta Chat".

Messenger and video services offer **various functions.** As part of the sector enquiry, the Bundeskartellamt asked the services which essential functions (here: Sending text messages, telephony, video telephony and sending files) consumers can use with their service and since when the offer has existed. More than 30 of the messenger and video services surveyed responded that users can send text messages, make phone calls, exchange video calls or send files via their service. However, for individual respondents in this group, consumers can only exchange information bilaterally via telephony and video telephony, not in groups. The survey results also show that the first functions were offered as early as 2000. Since then, more and more services and more and more functions have been added. Many services have offered the sending of text messages and files several years earlier than telephony and

---

55 Gematik has overall responsibility for the telematics infrastructure (TI), the central platform for digital applications in the German healthcare system. By defining and enforcing binding standards for services, components and applications in the TI, Gematik aims to ensure that this central infrastructure is and remains secure, efficient and user-friendly, cf. https://www.gematik.de/.

56 See *Gematik*, TI-Messenger, available at: https://www.gematik.de/anwendungen/ti-messenger.

57 The Internet Message Access Protocol (IMAP) is a network protocol that provides a network file system for e-mails, cf. *Wikipedia,* available at: https://de.wikipedia.org/wiki/Internet_Message_Access_Protocol.

58 The Simple Mail Transfer Protocol (SMTP) is a protocol of the Internet protocol family that is used to exchange e-mails in computer networks. It is primarily used to send and forward e-mails, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

59 Cf. for detailed explanations *Initiative freie Messenger*, available at: https://www.freie-messenger.de/sys_matrix/.

video telephony. In individual cases, it is also recognisable that the exchange in a group was only possible later than communication with a single interlocutor.

The majority of messenger and video services thus offer all essential **functions**, even if some focus on individual services, such as messaging with WhatsApp or video conferencing with Webex, Zoom and Microsoft Teams. For example, with many video conferencing providers, the messaging function is only part of the video function. A stand-alone chat service is not always operated. Some respondents also pointed out that they do not know whether the users use the service e.g. as a telephone conference or video conference, as the latter only differs by switching on the camera.

This results in countless **business models.** In addition to the main focus on messaging or video conferencing, platforms with messaging functions sometimes see themselves more as social networks or social media platforms (Facebook Messenger, Discord, WeChat) or as services for communication and collaboration (e.g. Slack, Rocket.chat). Software providers and developers of special software (e.g. Fastviewer) that offer help for self-help, i.e. support companies in operating their own communication or video system and also offer hosting services, for example, should also be mentioned here. These services, which go beyond the core of messaging and videoconferencing, were also included in the sector for the purposes of the sector enquiry.[60]

A further distinction can be made according to whether a messenger and video service focuses on **private or business customers.** Many video services, for example, have made it clear to the Bundeskartellamt that although they also offer a limited range of services free of charge, they mainly offer their products to business customers for a fee. However, according to most industry players, it is not possible to precisely quantify the ratio of private to business in their own user base. A larger number of respondents explained that they do not (cannot) record the distinction between business and private use, among other things because they generally refuse to track their users or because this information is only known to the respective service provider or server operator.

---

[60] In the consumer law sector enquiry pursuant to Section 32 e GWB, a market definition is not required. The explanations in this section are therefore not suitable for describing such a market, but serve to structure the sector.

Of the services that provided information or estimated it, around a third indicated that their service is used exclusively or almost exclusively for business, exclusively or almost exclusively for private use, or both for business and private use.

Not all messenger and video services can be used with every type of **end device and operating system.** 38 respondents stated that their service can be used with desktop/notebook/laptop. Via smartphone/tablet, 38 services can also be used. Via a web browser, only 16 of the services surveyed offer access according to their own information. Browsers that can be used include Safari, Firefox, Google Chrome, Internet Explorer, Microsoft Edge and Opera.

More than 30 each of the messenger and video services surveyed have stated that they are applicable with the operating systems Android, iOS/MacOS (Apple) and Windows respectively. More than 20 respondents have stated that their service can be used with Linux. The services that cannot be used with one or more of the major operating systems are essentially free messenger clients. These are based on a specific messaging system, such as XMPP or Matrix. Consumers can choose here from a large number of available clients of a system the application that best suits their needs, e.g. to use a specific operating system.

2. Financing and turnover

Only about two thirds of the services answered the questions on financing and turnover. Furthermore, the information on turnover and sources of funding could not be verified within the framework of the sector enquiry.

Messenger and video services were found to be most frequently funded by **charges for basic services** and revenues from **charges for additional services**. For most services, these sources of funding each accounted for 100% of revenue. Three services stated that they are financed entirely or predominantly by advertising. Two other industry participants generate most of their revenue through the sale of their app. Two free messenger clients have stated that they are mainly financed through donations.

It is striking that none of the services surveyed named revenue from data use/sharing for **personalised advertising** as a source of income, although this answer option was explicitly given.

As expected, **net sales in 2020** showed a wide range within the industry between zero euros and double-digit millions.

3. Usage figures

The Bundeskartellamt also asked the services surveyed to provide the usage figures for their messenger or video service in Germany - separately for text messages, telephony and video telephony or in total. Several services stated in response to this question that they do not collect the data in question, among other things because there is no country-specific recording, because the use takes place via different services or because a separation from other functions is not possible. For the other services, plausible data was provided, especially for the number of registered users and the average number of messages or minutes per day in 2020. In the following Figure 1, the services are named in alphabetical order, so that no conclusions can be drawn about the (relative) level of the respective usage figures. Services that do not appear in the overview either do not fall into the categories mentioned or have not provided any (plausible) information.

Number of users registered in 2020:	
50,000 to 1 million	Fastviewer, Ginlo, TeamViewer Meeting
1m to 25m	Discord, GoToWebinar, Line, Skype, Slack, Threema, Viber, Webex, Zoom
Over 25 m	Facebook Messenger, GoToMeeting, Snapchat, WhatsApp
Number of text messages sent on average per day in 2020:	
50,000 to 10 million	Delta Chat, GoToWebinar, Skype
10m to 100m	Discord, GoToMeeting, Microsoft Teams, Snapchat, Viber
Over 100 m	Facebook Messenger, WhatsApp
Number of telephone minutes used on average per day in 2020:	
50,000 to 1 million	GoToWebinar, Skype, Webex
1m to 20m	Facebook Messenger, GoToMeeting, Snapchat, Viber
Over 20 m	Discord, WhatsApp
Number of video minutes used on average per day in 2020:	
50,000 to 5 million	GoToWebinar, Snapchat, Webex
5 million to 25 million	Discord, Viber
Over 25 m	Facebook Messenger, WhatsApp

Figure 1: Usage figures

4. Competitive situation

In order to shed more light on the competitive situation, the Bundeskartellamt asked the messenger and video services about their own role in the market and their assessment of the competitive environment. The survey is not to be confused with a market definition under cartel law, which is not necessary for the sector enquiry under consumer law. Rather, the questions were designed to shed light on fundamental competitive contexts that could play a role in any recommendation for action under consumer law.

On the question of the **reasons why** users choose their respective messenger, the following questions were asked

/The majority of the industry players surveyed stated that the high level of data protection or data security of their service was a decisive factor in their choice. More than half of the services also consider their useful functions, the business functions and the free availability of their own service to be decisive for the choice of users. Only just under a third of the messenger and video services stated that they also gained their users because of their large user base.

Individual services have indicated that they operate within a fixed group (e.g. a department) and are therefore more secure, or that no registration is required to use their service. Therefore, there would be no network effects. According to some respondents, users also chose their service because of the ease of use, no advertising, integration with other systems/devices, infrastructure in Europe, design as an open source service, use of an international standard (XMPP) or because of the good quality of the service. One service explained that its users particularly appreciated the possibility to establish interoperability via bridges.

A further question concerned the **most important competitors of** the respective service including the corresponding justification. As was to be expected, the most important competitors were named in particular the large, well-known messenger or video services such as Facebook Messenger, Google Meet, Microsoft Teams, Signal, Skype, Slack, Webex, WhatsApp and Zoom (alphabetical order), whereby a distinction was to be made in each case between messengers and video conferencing providers. A leading service pointed out that basically every communication service is considered a competitor and that the exact designation of competitors is difficult without a concrete delineation of the relevant market.

In particular, comparable functions and similar target groups (users/advertising customers) of another service were named as **key competitive factors**

as well as the possibility of free use and a high level of awareness. The large number of users or the great market power of another service, on the other hand, were cited less frequently as competitive factors.

Several respondents pointed out that the messenger or video services from Microsoft (Microsoft Teams/Skype), Google (Google Meet) and Apple (iMessage/FaceTime) are coupled with other strong market applications or devices from the companies concerned (Office365, Google Workspace, iPhone). The users would have to make the decision and the

application is thus considerably "facilitated". One open source provider sees itself hindered by Microsoft Teams in this context. Market participants also pointed out several times that the original WhatsApp protocol was based on the XMPP standard. However, WhatsApp had not adopted its further development, but had designed a closed system based on it.

When asked about the **strategic goals of** their messenger or video service, some services mentioned the expansion of the user base, the expansion of paid functions, the increase of awareness or improvements in data protection, data security and quality. According to this, foreign services partly plan to focus more on the local offer. Small free messenger clients often have no plans to significantly expand their service. They have partly stated that they are not pursuing an economic interest. Improving interoperability with other services was also named by services as a goal.

Regarding the **competitive situation,** one service noted that only those messengers are used in politics that comply with IT standards (e.g. through corresponding specifications in tenders). Another service pointed out that it acts as a strong competition driver in the sector if users use several services in parallel (so-called multi-homing) and network effects are prevented if users can use other services (e.g. by invitation) without registering. Finally, one service emphasised the intense competition and the high competitive dynamics in this sector.

In addition to these assessments of the industry participants regarding the competitive situation in messenger and video services, we would like to refer at this point to the consumer survey conducted by the

Bundesnetzagentur (Federal Network Agency)[61] , which, among other things, recorded the proportion of respondents who use certain services:

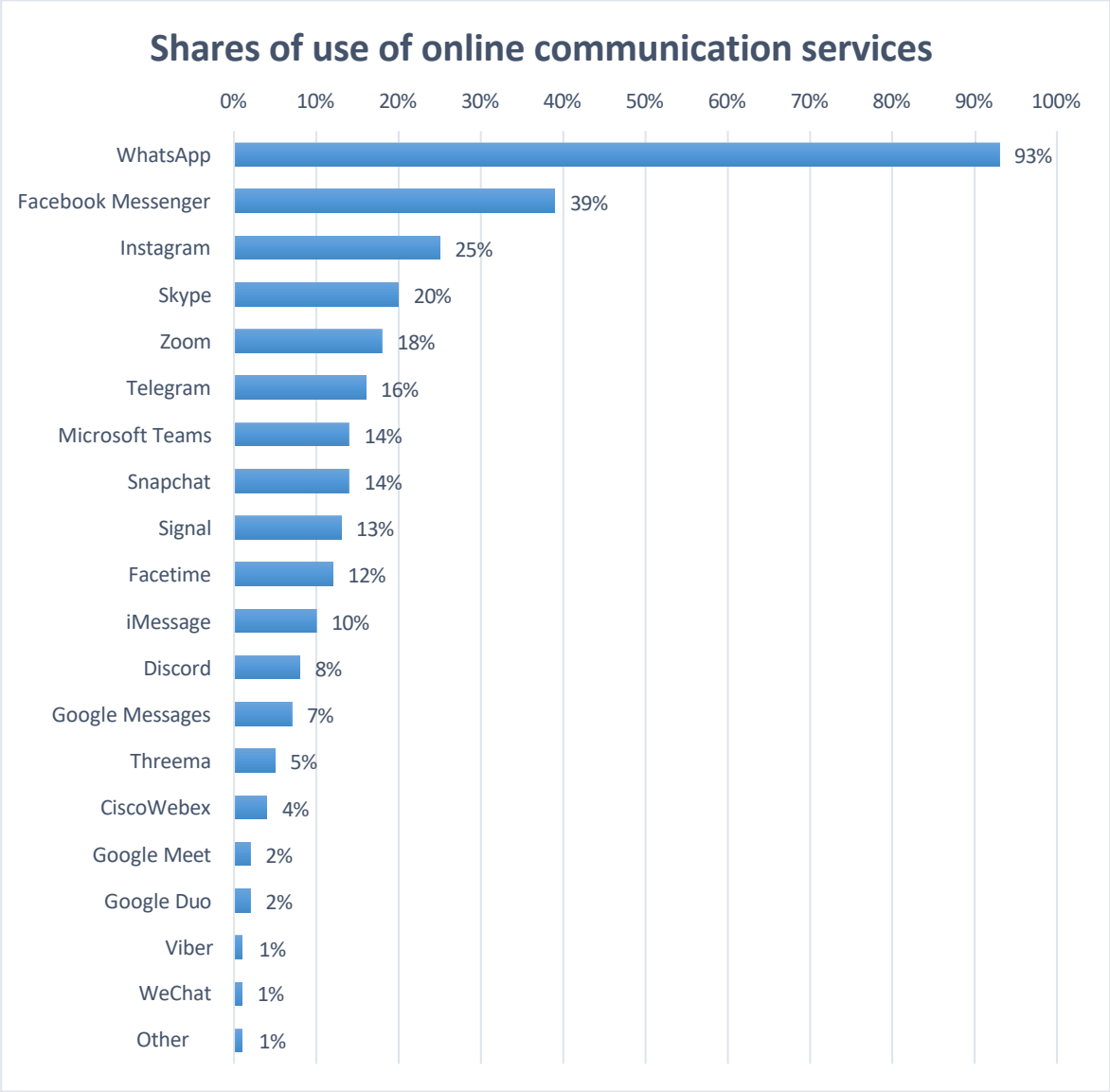


Figure 2: Usage shares of messenger and video services[62]

[61] *Bundesnetzagentur* (2022), Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_kurz21.pdf?__blob=publicatio nFile&v=3.

[62] Source: Own representation based on Bundesnetzagentur (2022), Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, p. 13.

Figure 2 illustrates that consumers' preferences for their choice of messenger and video services have hardly changed compared to the previous survey. WhatsApp is far ahead here with 93 percent, followed by Facebook Messenger with 39 percent. Among the services that consumers use primarily for messaging, Telegram and Signal are far behind WhatsApp with 16 and 13 percent usage shares, respectively. The leading video services are far behind the services from the Meta group with usage shares of less than 15 percent. Other messenger services follow far behind with single-digit usage shares. It seems that the lively competition in the industry described by the services has not touched the position of the leading service so far. A more detailed analysis of the competitive situation would require a market definition under cartel law, which is not necessary for the sector enquiry under consumer law - as already mentioned at the beginning.

D. Aspects of data protection in messenger and video services

The Bundeskartellamt directly questioned the messenger and video services for this sector enquiry in summer 2021. In its questionnaire, it devoted a separate section to the topics of data security and data processing in accordance with the EU General Data Protection Regulation (GDPR)[63] . Both topics are not only important for consumers to be able to independently choose a secure service. They also play a role in the legal analysis under the DSGVO and the UWG.

I. Data security

Consumers who are interested in the topic of data security in messenger and video services can now access numerous studies on this topic on the internet by consumer associations, IT bloggers or other informed circles.[64] The results presented in these studies are largely the result of evaluating publications or the websites of the messenger and video services included. The Bundeskartellamt directly asked the industry about its technical basis as well as its assessments of various data protection topics.

1. Network structure

a) Background

The influence of the respective messenger and video service as service operator is determined by the network structure, i.e. whether a messenger and video service is organised centrally via a specific server (see Figure 3) or federally via a network of independent servers (see Figure 4). In the case of **central organisation, there is a** server to which every user must log in, and a client (app, software) which is managed by the service operator.

---

63 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC, OJ EU L 119, 04.05.2016, p. 1 - GDPR.

64 Cf. e.g. For example, *Verbraucherzentrale NRW*, WhatsApp-Alternativen- Messenger im Vergleich, available at: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen- messenger-im-ueberblick-13055; *Mobilsicher*, Verschiedener Messenger-Apps kurz vorgestellt, available at: https://mobilsicher.de/suche/messenger; *Kuketz*, Messenger-Matrix, available at: https*://www.kuketz-blog.de/messenger-matrix-uebersicht-vergleich-der-aktuellen-messenger/; Initiative freie Messenger*, available at: https://www.freie-messenger.de/.

is provided. All essential decisions are thus in the hands of the service operator. The advantage of a centralised messenger and video service is, for example, the higher flexibility that is necessary in a rapidly changing ecosystem. The central service operator could react more quickly to changes and, for example, fix possible security gaps through central updates for all users at the same time.[65] In addition, there would be quality advantages. All users could always use the same version of the client because of the central server.

which would allow all users to benefit from the updated functions.

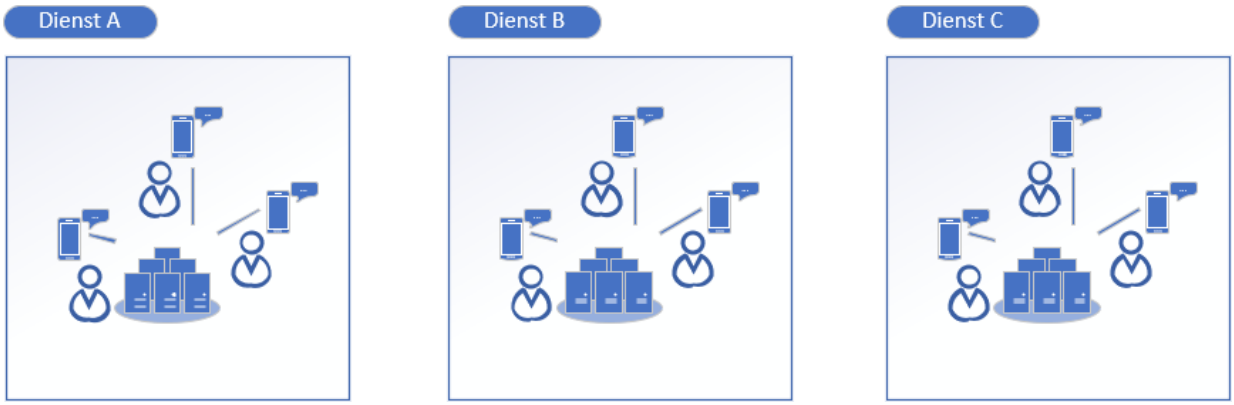


Figure 3: Centralised messaging systems[66]

With decentralised server organisation, the so-called **federation, the** servers of different server operators are linked together. A network of independent servers is formed, similar to the case with e-mail. The advantage here is that users can communicate with each other without being dependent on a central service provider. Furthermore, in federated systems, meta-data is not available at a central location, but only at the participating server operators, which users can select themselves if they wish. The two free protocols XMPP and Matrix, for example, enable federation.[67]

---

[65] See also, for example, *Bundesnetzagentur* (2021): Interoperability between messenger services - Overview of potentials and challenges, 9 December 2021, available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP.pdf? blob=publicationFile&v=3.

[66] In accordance with *Bundesnetzagentur* (2021): Interoperability between messenger services - overview of potentials and challenges, 9. December 2021, available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digital/OnlineKom/discussion_paper_IOP.pdf? blob=publicationFile&v=3.

[67] Cf. *Kuketz*: Die verrückte Welt der Messenger - Teil 1, p. 5, available at: https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/.

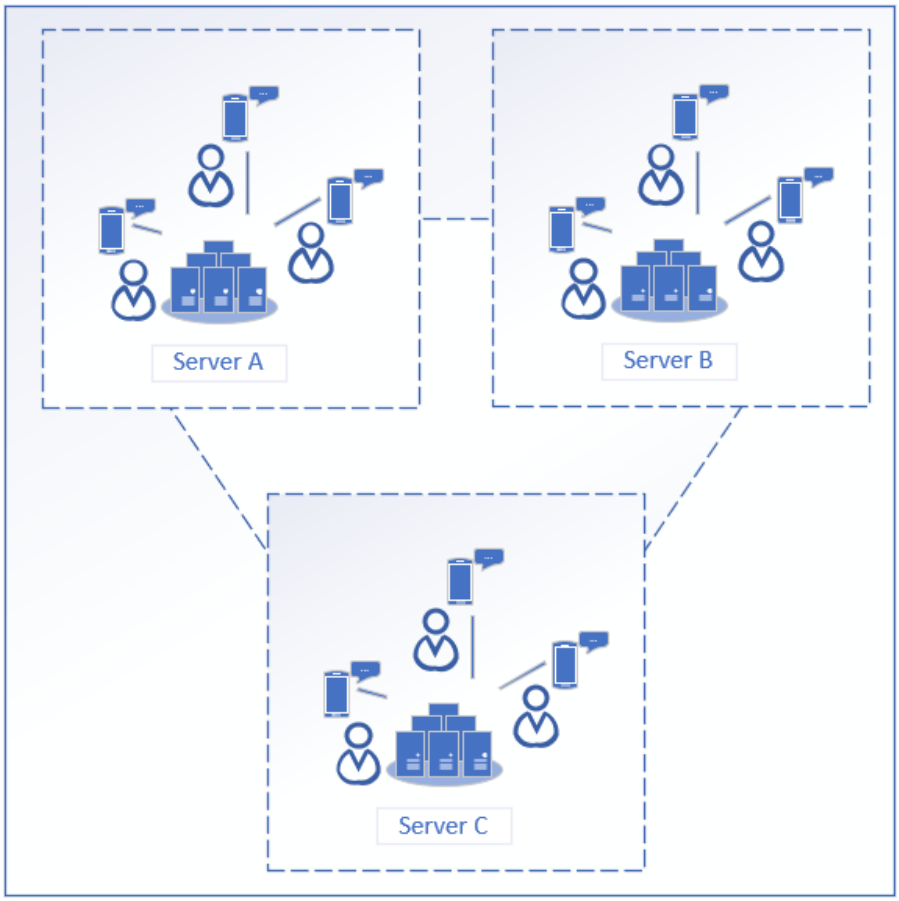


Figure 4: Federated messaging system[68]

b) Investigation results

The majority of messenger and video services have indicated that the underlying network structure is centrally managed, mostly by their own company.

A federated server structure is used by more than 40 per cent of the services. These include, for example, BigBlueButton, Blabber.im, Conversations, Delta Chat, Discord (only for video/VOIP), Element, Fastviewer,

iMessage / FaceTime, Jabber, Monal, Nextcloud Talk, Quicksy, Rocket.Chat, Trillian, Yaxim, Viber.

Two free messenger clients point out that the system (XMPP) is usually operated in a decentralised and federated manner - however, it is also often used, for example, as an isolated (centralised) solution within a company.

[68] In accordance with *Bundesnetzagentur* (2021): Interoperability between messenger services - overview of potentials and challenges, 9. December 2021, available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digital/OnlineKom/discussion_paper_IOP.pdf? blob=publicationFile&v=3

comes into play. Furthermore, serverless communication is also possible with corresponding restrictions. Which of these structures is used is up to the end users. Several XMPP clients also point out that some closed messaging systems have emerged on the basis of XMPP. This concerns Facebook Messenger as well as WhatsApp, Google Talk and KIK Messenger. This means that the companies involved used the standardised and public protocol XMPP (and "ejabberd" as one of the freely available open source server implementations of XMPP) to create their product on its basis through proprietary (company-internal) extensions that they did not allow to flow back into the public standardisation process.

2. Cooperation with standardisation organisations

a) Background

In line with the importance of technical functionalities, the industry of messenger and video services also has a certain technical self-organisation through internationally recognised standardisation organisations. In principle, standardisation organisations adopt internal rules for dealing with proprietary technologies (see again C.III).
When messenger and video services use techniques that have been standardised and documented by the industry in standardisation bodies, the advantages for users are that an industry-recognised technical standard is implemented that has become established on the market and has been assessed and tested by a wide range of users.

b) Investigation results

Just under half of the services have confirmed cooperation with standardisation organisations. These include the services that use a standardised protocol, such as the XMPP clients that cooperate with the XSF, the Matrix.org Foundation and also Delta Chat, Google Meet, Meet.jit.si, Loopup, Slack, Swyx, Threema, Tixeo, Webex, Zoom.
Among the standardisation organisations, the **Internet Engineering Task Force (IETF)** is very often mentioned. Its focus - as described in Chapter C.III - is on the standardisation of the communication protocols used on the Internet. The IETF is an open, international voluntary association of network engineers, manufacturers, network operators, researchers and users that is concerned with the technical development of the internet in order to improve its functioning.

In addition, there are other standardisation bodies that are particularly important for the services, or even certain groups of the services. The organisation **XMPP Standards Foundation (XSF)** has been named by many free messenger clients. The XSF is a non-profit foundation that specifies and further develops the XMPP protocol. The open standard Matrix is developed by the foundation **"The Matrix.org Foundation**".

Other mentions were the ISO, NIST, ANSSI, W3C, the OpenPGP Working Group or the Autocrypt.org standardisation community:

The **International Organisation for Standardisation (ISO)** is the international association of standards organisations. It develops international standards in all areas except electrics and electronics, for which the International Electrotechnical Commission (IEC) is responsible, and except telecommunications, which is dealt with by the International Telecommunication Union (ITU).

In keeping with the international nature of the business, the services also name foreign authorities that perform similar tasks to those performed by the BSI in Germany. The **National Institute of Standards and Technology (NIST)** is a federal authority in the business area of the United States Department of Commerce with headquarters in Gaithersburg (Maryland). The institute publishes the Federal Information Processing Standards (FIPS) that apply to US authorities and is responsible for standardisation processes. In the field of cryptography, for example, the DES and AES encryption algorithms should be mentioned here. The **Agence nationale de la sécurité des systèmes d'information (ANSSI)** is the French authority responsible for information security. It is attached to the General Secretariat for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale, SGDSN), which reports directly to the French Prime Minister.

The **World Wide Web Consortium (W3C)** is a membership organisation for standardising techniques on the World Wide Web. Some respondents pointed out that the W3C was instrumental in developing the WebRTC standard. This is an open standard that defines a collection of communication protocols and application programming interfaces (API) that enable real-time communication over computer-to-computer connections. Applications such as video conferencing, file transfer, chat and screen sharing can function in this way.

The **OpenPGP Working Group** is a working group at the IETF that worked on the standardisation of the most widely used encryption standard for emails "OpenPGP". **Autocrypt.org** is a standardisation guideline for implementing end-to-end encryption of e-mails.

3. Standards / Protocols

a) Background

Communication protocols define the rules for data transmission between the end points of communication. They can be described as the language of a messaging and video system or - formulated more technically - as a set of rules according to which the data transmission between two or more end points of the communication takes place. A communication protocol thus defines specifications for the transmission of data between communication partners. The **programming interface** or API (Application Programming Interface) is provided by the software for linking to the respective system.[69] The protocol also regulates **encryption**, which is described separately below due to the complexity of the topic and its particular importance for interoperability and legal issues (see D.I.4.).

As part of the survey, the messenger and video services were to inform the Bundeskartellamt whether they use their own, so-called **proprietary** protocols. Proprietary is the term used for software and hardware or file formats, protocols or programming interfaces (APIs) which are based on manufacturer-specific developments and which can be used in a restricted manner due to legal regulations (patents, licensing regulations) or whose source code is not available. Reference should be made here to the process of innovation, diffusion and standardisation. Innovation in this case is driven by the economy. The innovations are reflected in the details of the protocols and these then in the development of the necessary programmes (source code). These developments are first the intellectual property of the services. The protocol specification is the important level, as it aims to ensure the interoperability of different implementations. Ideally, the standards then develop from this, and only those functions that have become established in the market find their way into them.

Whether proprietary - as is customary in common parlance - also indicates an existing ownership relationship here is not clearly clarified. In contrast to this, **open source**

[69] See chapter F.I.3 for the API.

products can be studied, used, modified and copied by anyone at will.[70] Their source code is open.[71] Proprietary protocols can therefore not or not completely be checked by third parties for their respective functioning. If the source code of proprietary protocols is disclosed, at least expert users or testing institutions can understand their design and determine, for example, in what form a messenger or video service encrypts content end-to-end. In the past, for example, it became known that one service advertised end-to-end encryption, although it was actually "only" transport encrypted.[72] According to the BSI, it is comparatively easy to verify such statements in open source products. However, the BSI also points out the high demands of such projects, since modern messenger and video services have an "enormous amount of source code"[73] .

If the source code is not open or users cannot or do not want to check their service themselves, **certifications** or **security audits can be** helpful in assessing data security and increasing trust in it. In this context, the BSI refers to independently conducted security audits, certification of the provider according to ISO 27001 or publication of the cryptographic design criteria.[74]

b) Investigation results

The Bundeskartellamt has asked the messenger and video services for information on which protocols/standards they use for the exchange, to what extent the source codes are publicly accessible and to what extent they are available to the public.

---

70 See *IT-Business*, available at: https://www.it-business.de/was-ist-proprietaer-a-911656/, Stand: 19 January 2022. Also explained, for example, on *Wikipedia*, available at: https://de.wikipedia.org/wiki/Open_Source.

71 Cf. *Bundeszentrale für politische Bildung*: Dossier Open Source, available at: https://www.bpb.de/gesellschaft/digitales/opensource/, *Red Hat*: Was ist Open Source, available at: https://www.redhat.com/de/topics/open-source/what-is-open-source#, *Chip*: Open Source - was ist das genau?, available at: https://praxistipps.chip.de/open-source-was-ist-das-genau_12877.

72 See also chapter D.III.4.d.bb.

73 *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

74 *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

or whether they are proprietary and proprietary protocols, and whether the protocols are regularly reviewed. Many of the respondents mentioned transport encryption (TLS)[75] , the Web Real-Time Communication standard (WebRTC)[76] , which is used for video communication, the Extensible Messaging and Presence Protocol (XMPP)[77] , the Double Ratchet protocol, the Matrix protocol, which is based on Double Ratchet, as well as AES (see chapter D.I.4.a. for both) and SIP[78] as the protocols or standards used.

aa) Visibility of the source codes / open source

Slightly more than 40 per cent of the services surveyed stated that the source code of the server and client can be viewed (All-in-One Messenger, BigBlueButton, Blabber.im, Conversations, Delta.Chat, Dino, Element, Gajim, Google Meet, Jabber, Meet.jit.si, Monal, Nextcloud Talk, Quicksy, Rocket.Chat, Swyx, Threema, Univado, Yaxim). This is especially the case with the free messenger clients and, of course, open source services. This also includes services that explicitly advertise data protection.
In the case of the **free messenger clients, a** distinction must be made between the "client" and the "system" (especially the protocol) when classifying them in the above-mentioned categories. The XMPP protocol, which some of the free messenger clients surveyed use, is open source, i.e. the source code is available in the open and can be viewed and used by anyone. The protocol has been standardised by XSF. However, there are both open source and proprietary, commercial servers and clients.
For example, the XMPP clients Blabber.im and Yaxim point out that the servers they use are also open source. Other clients state that open-source servers can be chosen by the users (Dino, Gajim). Also the client Delta Chat, which uses the servers required for email

---

75 TLS (Transport Layer Security) is an encryption protocol for secure data transmission on the Internet; also known by its predecessor name Secure Sockets Layer (see SSL certificate).

76 WebRTC (Web Real-Time Communication) is an open standard that defines a collection of communication protocols and application programming interfaces (API) that enable real-time communication over computer-to-computer connections.

77 XMPP (Extensible Messaging and Presence Protocol) is an open standard of a communication protocol published by the Internet Engineering Task Force (IETF) as RFC 6120, 6121 and 6122. XMPP is based on the XML standard and enables the exchange of data, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol.

78 SIP stands for Session Initiation Protocol, a protocol to make phone calls over the internet, for more details see: https://www.computerlexikon.com/begriff-sip.

explains that the source code of many email servers is visible, but that of other email servers it is not. However, it is possible for users to choose a server with open source code without restrictions or, if in doubt, to operate one themselves. The Matrix.org Foundation also confirms that the Matrix protocol is open source.

However, open source does not mean that the service or all functions of the service are available to consumers free of charge. Rather, there are also **paid solutions**. Nextcloud is a software producer whose customers operate Nextcloud (Talk) on their own servers. Nextcloud Talk is based on WebRTC and is **open source** software that can be downloaded from the website. Since Nextcloud is freely available, as are the apps, the service says it sells "Nextcloud Enterprise", a "software for enterprises, which also includes support". The Rocket.Chat "platform" states that the client and server code is open source, as are the features for business users, even if they are not available for free. Meet.jit.si uses the Jitsi Meet open source software for video conferencing, which is based on the WebRTC standard, among other things. Meet.jit.si is hosted by the company 8x8.

Google Meet explains that the service uses the free open source standard WebRTC, which was published by Google in 2011 as an open source project. The specifications were published by the World Wide Web Consortium (W3C) and the IETF. Threema, a service that advertises numerous data security and data protection measures for a fee, also discloses its source code.

bb) Proprietary and open source

About a third of the services declared their used protocols as proprietary and company property. These include well-known services such as Discord, Line, Tixeo, TeamViewer Meeting, Viber, Webex, WhatsApp, Zoom.

Some messenger and video services use both **proprietary and open source protocols**. Adobe has developed its own proprietary network protocol, RTMP[79] . There are open source implementations of the protocol; however, the implementation in "Adobe Connect" is "closed source". GotoMeeting and GotoWebinar use a mix of proprietary and standardised protocols (TLS, HTTP, WSS, RTC, WebRTC) to provide secure communication via audio and video telephony as well as screen sharing and chat. Skype also claims to use TLS and the Double Ratchet protocol, but also uses its own protocol and TLS. Viber also refers to the Double Ratchet-

[79] Cf. *Wikipedia*, available at: https://en.wikipedia.org/wiki/Real-Time_Messaging_Protocol.

protocol, as used in the "Open Whisper[80] signal application. This is the basis of Viber's end-to-end encryption. However, Viber's implementation is new from scratch and does not use Signal's source code. Trillian realises its actual service via its own protocol "IMPP". Documentation on IMPP is available online.[81] However, federation works with XMPP.

cc) Security audits / app testing

A good 40 percent of the services stated that the source code of the server and client is regularly evaluated by independent security audits and app testing (e.g. Conferencing & Collaboration, Conversations, Delta Chat, Discord, Franz, Google Meet, Meet.jit.si, Loopup, Nextcloud Talk, Quicksy, Rocket.Chat, TeamViewer Meeting, Tixeo, The Matrix.org Foundation, Threema, Webex, WhatsApp, Zoom.). This also includes many of the services that call their protocol proprietary.
Two services explain that the source codes of the server and client could only be viewed by way of an effective confidentiality agreement. However, they are regularly evaluated by independent security audits and app tests.
The type of inspections and the corresponding occasions vary greatly across the sector. Often, several **measures** are **combined**. These measures can be **internal or external**. For example, it is explained that a penetration test[82] and a security audit by an external body are carried out annually. A leading video service explains that an expert evaluates the products and services at least once a year. Another service states that the source code is regularly evaluated before a new version is released. Different services

---

80 Open Whisper System was a software company that began developing the Signal messenger protocol and app. It went into the non-profit Signal Technology Foundation, through which Signal has been developed since 2018. The official servers are operated by a subsidiary of the foundation, Signal Messenger LLC, cf. *IT-Times*: Signal - was hinter dem-beliebten-instant-messenger-steckt-132617/ and *Wikipedia*, available at: https://en.wikipedia.org/wiki/Open_Whisper_Systems.

81 Cf. Trillian, available at: https://trillian.im/impp/.

82 A penetration test is a targeted, permitted attempt to penetrate IT systems in order to improve IT security, see e.g. *itexperts,* available at: https://www.itexperst.at/penetrationstest- definition-abgrenzung-ueberblick .

refer to so-called **bug bounty programmes**[83,] e.g. also to "HackerOne"[84] to identify vulnerabilities and attack points of their system. A widely used video service explains that the source codes of the server and client are regularly evaluated by internal and external security experts. The internal checks are constantly running and are automated and carried out manually via the SAST procedure[85] .
The name of the verifying institution and whether the corresponding reports are public was only given in isolated cases. For example, the French National **Agency for Information Systems Security (ANSSI**) and the CSPN - Standard certified by it are mentioned. The "Certification de Sécurité de Premier Niveau" (CSPN) was created by the French ANSSI to provide an alternative to the assessments of the internationally recognised CC (Common Criteria) certification .[8687] Tixeo points out that as of 15 June 2022**,** the **immediate, reciprocal**

---

[83] A bug bounty programme is an initiative run by companies, interest groups, private individuals or government agencies to identify, fix and publicise bugs in software by offering non-cash or cash prizes to the discoverers, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Bug-Bounty-Programm.

[84] HackerOne is a vulnerability coordination and bug bounty platform that connects companies with penetration testers and cybersecurity researchers. It is considered the largest cybersecurity company of its kind. As of May 2020, *HackerOne*'s network had paid $100 million in bounties, see *Wikipedia*, available at: https://en.wikipedia.org/wiki/HackerOne and *HackerOne*, available at: https://www.hackerone.com/.

[85] Static Application Security Testing (SAST) is a way to automatically test and analyse the source code of a programme without executing it, in order to detect security vulnerabilities early in the software development cycle. Security checks are done early in development, see *Dev-Insider*, available at: https://www.dev-insider.de/was-ist-sast-a-1002595/ and *Parasoft*, available at: https://de.parasoft.com/blog/what-is-sast-static-application-security- testing/.

[86] The Common Criteria are an international standard for testing and evaluating the security features of IT products.

[87] The tests are carried out in a limited time and with a limited amount of work (typically two months, 25 to 35 person days. cf. *Stormshield*, Qualified security solutions - the decision for a trustworthy solution, available at: https://www.stormshield.com/de/ news/qualified-security-solutions-the-decision-for-a-trustworthy-solution/.

Recognition of IT Security Certificates between ANSSI and BSI was agreed.[88] With the entry into force of the agreement, certificates already valid in both programmes will be recognised as equivalent. Certificates issued in the future will be automatically recognised upon their publication.
Tixeo has received renewed CSPN certification from the ANSSI for its standard end-to-end certification 2021. This means that the CSPN certification is now also valid for Germany. Individual services also refer to standards from ISO and the BSI.
One free messenger client has already conducted two external security audits as part of funding programmes, and expects more in the future. Another free client explained that due to the poor donation/funding situation, there was no money for independent safety audits. This was linked to the desire for grants or directly funded audits.

4. Encryption

a) Background

The topic of encryption is now being discussed intensively not only in the professional public, but also in the general consumer public. However, the encryption of messages is already subject to a long development process that is continuing.

aa) Procedure

In the 1990s, messages were still sent unencrypted, e.g. with the chat programme ICQ. Nowadays, with so-called **transport encryption,** the message is encrypted during its transport (encrypted channel), but is unencrypted outside the transmission path and at the end points, i.e. it can be viewed both by users of the messenger and video service themselves and by the server operator. The technology used is the "Transport Layer Security" standard, which has existed since 1994.

In contrast to transport encryption, **end-to-end encryption ("E2E encryption")** encrypts the message and thus transmits it across all transmission stations.

---

[88] The former President of the Federal Office for Information Security (BSI), Arne Schönbohm, and the Director General of ANSSI, Guillaume Poupard, have signed an agreement on the mutual recognition of IT security certificates. The agreement relates to the CSPN (Certification de Sécurité de Premier Niveau) and BSZ (Accelerated Security Certification) programmes. Cf. BSI, Mutual Recognition of IT Security Certificates between ANSSI and BSI, available at: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/ANSSI_BSI_IT-Sicherheitszertifikate_220615.html.

sent. Only the communication partners as end points of the communication can decrypt the data. Accordingly, from a theoretical perspective, a combined use of transport and end-to-end encryption offers the greatest security, regardless of individual cases (see Figure 5).

The combined use of both encryption methods can be illustrated if the content of a message to be encrypted is compared with an item that is checked in at the airport. With transport encryption, the luggage is protected in the fuselage of the aircraft during the flight. There it is not accessible during the flight. However, upon departure and arrival at the airport, anyone can then access the item. An end-to-end encrypted item is packed into a secure container on departure, which can only be opened again by the owner on arrival. Not only during the flight, but also before and after, no third parties can access the luggage or the encrypted contents.
access.[89]

Various cryptographic methods such as symmetric or asymmetric encryption with public and private keys are used for encryption.
The difference between symmetric encryption and asymmetric encryption lies in the number of keys. In symmetric **cryptography, the** same key is used for encryption and decryption. This results in the key exchange problem. In order for a communication partner to decrypt the encrypted message, he must know the key that was also used for encryption. If a third party listens in on the communication channel during the transmission of the key, this third party could then decrypt the entire communication or send encrypted messages themselves without being noticed. Therefore, the key transmission must be secret, which is often a problem due to physical distances.

[89] Cf. *CYQUEO*: End-to-end encryption and transport encryption - what's the difference?, available at: https://cyqueo.com/magazin/ende-zu-ende-verschluesselung-und- transportverschluesselung-was-ist-der-unterschied/.

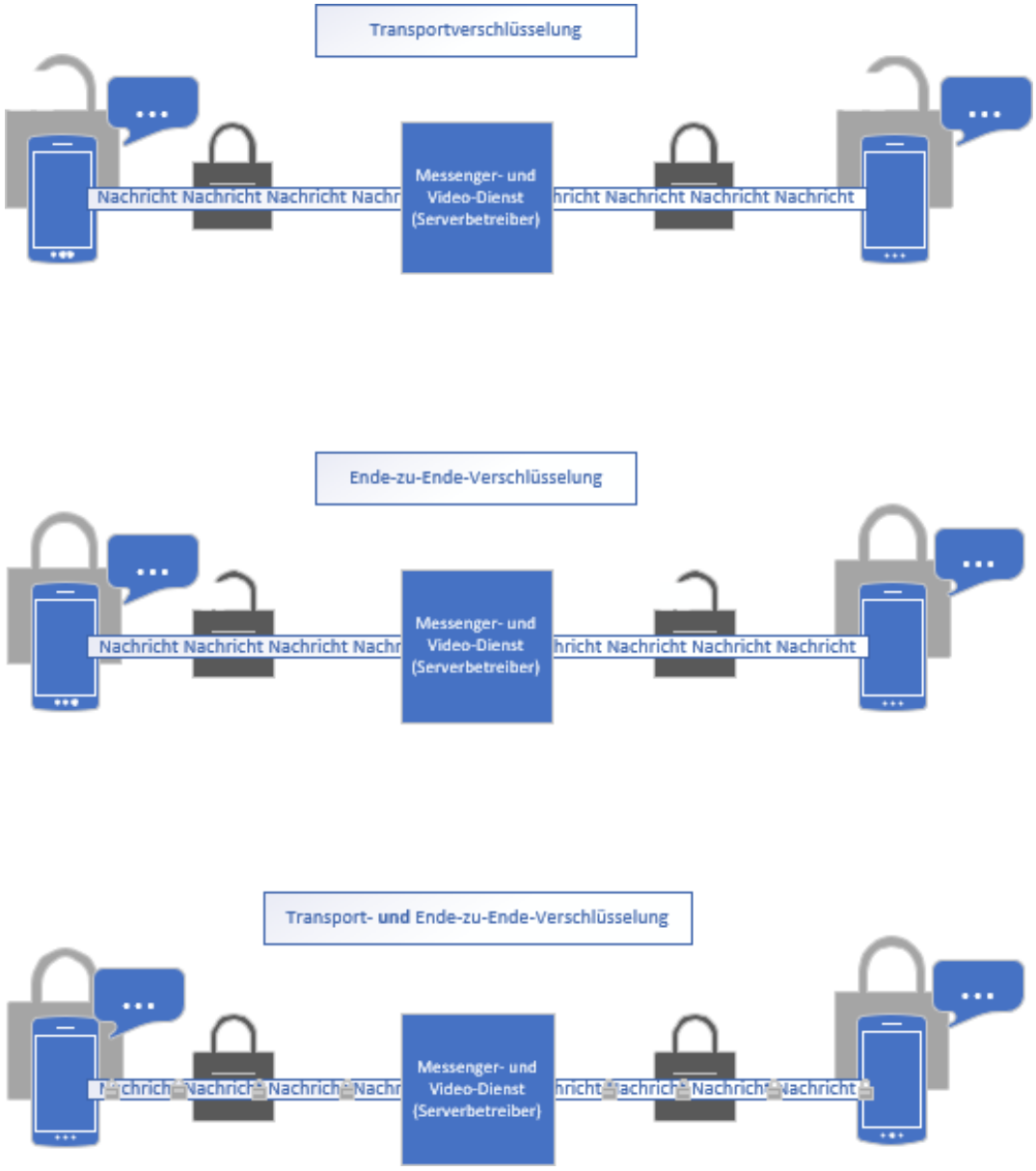


Figure 5: Transport and end-to-end encryption separately and combined[90]

A well-known symmetrical encryption method is the **Advanced Encryption Standard (AES)**. The standard is usually implemented together with other encryption methods, e.g.

[90] Own presentation based on *Initiative freie Messenger*, Verschlüsselungsarten und Kombinationsmöglichkeiten, available at: https://www.freie-messenger.de/dateien/begriffe/Verschl%C3%BCsselung.PDF.

also as the basis of transport encryption. The AES encryption method is a block cipher[91] whose block size depends on the AES encryption variant. The variants of AES encryption, AES-128, AES-192 and AES-256, contain the length of the key in bits in their designation. The most secure AES variant is therefore AES-256.[92]

In contrast, **asymmetric encryption has** two keys. The message is encrypted with one key and decrypted again with the other key. The encryption key is publicly accessible and does not have to be transmitted secretly, as is the case with symmetric encryption. The second key is the private key that the recipient uses for decryption. In the best case, only the recipient is in possession of the private key.[93] A well-known asymmetric encryption method is the **RSA method** (named after the developers R. Rivest, A. Shamir and L. Adleman). With the RSA method, digital data can be converted and made unrecognisable using a specific algorithm. The so-called RSA key is necessary for decryption. However, the same key is not used for encryption and decryption, but a key pair consisting of a private and a public key. The private key must be kept secret for secure RSA encryption.[94]

Finally, the security of communication is determined by further cryptographic principles and properties. "**Authenticity**" means that the originator of data or the sender of a message should be clearly identifiable and his or her authorship verifiable. The following properties of cryptographic data are also worthy of mention

Protocols: "**(Perfect) Forward Secrecy**" makes it impossible to reconstruct a session key by knowing a secret master or long-term key. A recorded encrypted communication can thus not be decrypted retrospectively even if the long-term key is known.

"**Backward Secrecy**" ("Future Secrecy", "Post-Compromise Security") guarantees that encrypted

---

91 Cf. *Chip*, AES Verschlüsselung: Standard einfach erklärt, available at: https://praxistipps.chip.de/aes-verschluesselung-standard-einfach-erklaert_121070. A block cipher divides data to be encrypted into fixed block sizes. Their contents are mixed and shifted in several rounds.

92 See e.g. *Studiflix*, available at: https://studyflix.de/informatik/aes-verschlusselung-1611 as well as *Wikipedia*, available at: https://de.wikipedia.org/wiki/Advanced_Encryption_Standard.

93 See *Studiflix*, available at: https://studyflix.de/informatik/symmetrische-verschlusselung-1610.

94 See *Datenschutz.org*, available at: https://www.datenschutz.org/rsa-verschluesselung/.

Messages remain secret even after a key has been compromised in the past.[95] (Plausible) **deniability** makes it possible to credibly deny sending a message afterwards.

bb) Implementation of end-to-end encryption

End-to-end encryption is implemented using different procedures, depending on which form of communication is used. For example, OpenPGP[96] and S/MIME[97] are used to encrypt e-mails. For text messages, the so-called **double ratchet protocol**[98] (often also called signal protocol) is considered state of the art. It also implements the cryptographic principles described in the previous section. As the BSI explains, one of the basic ideas of the protocol is to **always** send **new (session) keys** with every message sent and to delete the old ones. The key material is thus "ratchet forward" so that it is not possible for an attacker to learn from a later key.
to return to an earlier point in time and decode previous messages"[99] .
The double ratchet protocol thus implements **asymmetric public key encryption:** When, for example, user A starts the app of his messenger service, a private and a public key are generated. The private key remains on the end device of user A. The public key is stored on the server for everyone who wants to send A a message. When user B writes to user A, her message is encrypted with A's public key so that only A can read the message.

---

95 Cf. *Kuketz*, Die verrückte Welt der Messenger - Teil 1, p. 4, available at: https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/.

96 OpenPGP is a standardised data format for encrypted and digitally signed data. It also defines the format of certificates, commonly referred to as "keys", see *Wikipedia*, available at: https://de.wikipedia.org/wiki/OpenPGP.

97 Secure / Multipurpose Internet Mail Extensions (S/MIME) is a standard for encrypting and signing MIME objects using an asymmetric cryptosystem. A typical use case is e.g. e-mail, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/S/MIME.

98 Cryptographic protocol for an asynchronous (i.e. the communication partners do not have to be online at the same time) end-to-end encrypted message exchange, see *Wikipedia*, available at: https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm or also in detail *Signal*: The Double Ratchet Algorithm, available at: https://signal.org/docs/specifications/doubleratchet/.

99 *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html and the literature cited there.

can decrypt the message and thus read it. The encrypted document is sent to A via the server. A receives the document, which is decrypted with his private key.[100] The content of the message cannot therefore be read by third parties, not even by the messenger and video service itself (see figure 6):

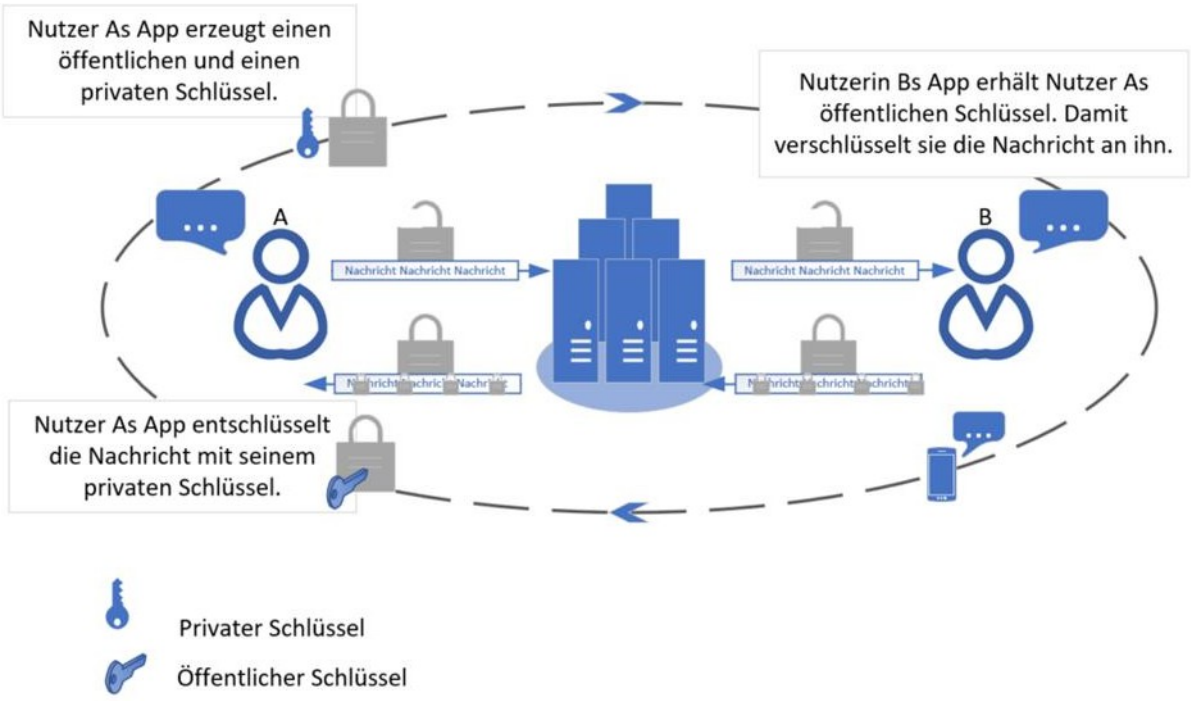


Figure 6: Asymmetric encryption[101]

The free messaging systems XMPP and Matrix also use an implementation of the double ratchet protocol for encryption, which enables forward secrecy, credible deniability as well as synchronisation of messages when the clients involved are offline.

The corresponding procedure in XMPP is **OMEMO (OMEMO Multi-End Message and Object Encryption)**, an extension for secure multi-client end-to-end encryption in bilateral

[100] It should be noted again that the private keys are continually renegotiated to achieve the cryptographic properties of Perfect Forward Secrecy, Backward Secrecy, and (Plausible) Deniability.

[101] Own presentation based on *Mobilsicher*, Das asymmetrische Verschlüsselungsverfahren, available at: https://mobilsicher.de/ratgeber/ende-zu-ende-verschluesselung-einfach-erklaert.

Exchange via text messages ("chat"). It is an open standard that can be used by all users.
users can be freely used and implemented.[102]

In **Matrix,** encryption is based on the "Olm and Libolm algorithms". In Matrix, a room is created for a chat regardless of the number of participants. Chat rooms are synchronised between the participating servers.[103] An optional end-to-end encryption from room to room is then realised by Olm using a double ratchet algorithm implementation.

This means that stored conversation data can only be read by room participants. If this is configured, data transported via Matrix is only visible to Matrix servers as encrypted text. It can only be read by authorised participants in the room.

be. With "Megolm", there is an Olm extension for larger chat rooms. Both were tested in a cryptographic review by the company NCC Group and the results were published and addressed by the Matrix team.[104] The review was funded by the Open Technology Fund .[105][106]

---

[102] Cf. Conservation, available at: https://conversations.im/omemo/, cf. XMPP, available at: https://xmpp.org/extensions/xep-0384.html. Overviews are available on the Internet that provide information on the extent to which encryption technology has already been integrated into the various clients, see Omemo-Top https://omemo.top/.

[103] All Matrix servers involved in a communication store the chat history indefinitely. On the own matrix server (home server), a message can be deleted if desired. The home server will forward this deletion request to all matrix servers that were involved in the communication after a renewed confirmation. However, it is uncertain whether the deletion request will be implemented on the other matrix servers involved, cf. *Kuketz* IT Security, Element: Messaging über die Matrix - Messenger Teil 7, available at: https://www.kuketz- blog.de/element-messaging-ueber-die-matrix-messenger-teil7/.

[104] See *NCC Group*: Olm cryptographic review, available at: https://pentestreports.com/ reports/iSEC/NCC_Group_Olm_Cryptogrpahic_Review_2016_11_01.pdf and Matrix.*org*, Matrix's 'Olm' End-to-end Encryption security assessment released**,** available at: https://matrix.org/ blog/2016/11/21/matrixs-olm-end-to-end-encryption-security-assessment-released-and-implemented-cross-platform-on-riot-at-last.

[105] Cf. https://www.opentech.fund/. According to its own information, the *Open Technology Fund (OTF) is* an independent non-profit organisation dedicated to promoting global internet freedom. OTF supports projects that counteract repressive censorship and surveillance to enable citizens worldwide to exercise their basic human rights online.

[106] See *Wikipedia*, available at: https://de.wikipedia.org/wiki/Matrix_(communication protocol).

For the **encryption of audio/video chats and SIP telephony**, the WebRTC protocol is usually used in combination with DTLS-SRTP (Datagram Transport Layer Security - Secure Real-Time Transport Protocol).[107][108] **WebRTC** (Web Real Time Communication) is an open standard that defines a collection of communication protocols and programming interfaces (API) that enable real-time communication via computer-to-computer connections.[109] All interested parties can access, use and further develop an "open standard". WebRTC has been standardised by the World Wide Web Consortium (W3C) and the IETF. Web Real Time Communication is based on the programming languages HTML (Hyper Text Markup Language) and JavaScript. They are read and played back by the respective web browser, regardless of which browser is used. This enables communication between several computers on the web and all users can make use of the transfer of data such as videos, documents or photos via the browser.[110]

---

[107] The Secure Real-Time Transport Protocol is the encrypted variant of the Real-Time Transport Protocol (RTP). The protocol was introduced by the Internet Engineering Task Force (IETF) in March 2004. It is particularly suitable for the encrypted transmission of communication via the Internet and is also increasingly used in IP telephony. The cryptosystem uses the Advanced Encryption Standard (AES). Depending on the implementation, the protocol can be used either for transport encryption during voice data transmission between an end device on the customer side and the server of the communication provider or for complete end-to-end encryption between communication partners, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Secure_Real-_Time_Transport_Protocol.

[108] Cf. *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

[109] Cf. *NordVPN*: What is WebRTC and how to deactivate it, available at: https://nordvpn.com/de/blog/was-ist-webrtc/.

[110] Cf. *NordVPN*: What is WebRTC and how to deactivate it, available at: https://nordvpn.com/de/blog/was-ist-webrtc/ as well as *Placetel*: WebRTC - definition, function and everything important about the application, available at: https://www.placetel.de/ratgeber/webrtc. The Secure Real-Time Transport Protocol (SRTP) is used for the audio-visual transmission of real-time communication via the browser. It is also used for IP telephony. The encrypted connection is guaranteed by the encryption protocol DTLS (Datagram Transport Layer Security).

cc) Technical limitations of end-to-end encryption

The encryption of **text messages in groups** is still considered complex and depends on the size of the group. The exchange in groups is currently encrypted by encrypting all individual chats between all group members. As the BSI states in its publication
"Modern Messengers" shows that the encryption effort grows quadratically with the number of Participant. "The quadratic overhead of encrypting group chats represents one of the main reasons that led to the founding of an IETF working group that has been working on a further development of the double ratchet protocol, the **Messaging Layer Security protocol (MLS),** which is intended to enable efficient group handling in particular"[111] . According to the IETF, a draft version of MLS is currently used by Webex, for example. Other services (including Matrix) planned to use MLS. The MIMI working group of the IETF, which has been active since the beginning of 2023, also takes MLS into account in its solutions for interoperable messaging.[112]
End-to-end encryption is also currently subject to technical limitations in **videoconferencing and webinars. In** general, end-to-end encryption requires that participants are technically capable of providing and applying the necessary encryption functions. All participants must be on the same security level. Conversely, E2E encryption cannot be achieved as soon as one participant falls below the required security level.
This occurs, for example, when participants use a **WebRTC client.** WebRTC is a protocol directly anchored in the browser, which can only encrypt end-to-end between two end points. If there are more than two participants in a videoconference, these are the end device of the user with the server of the service, which no longer meets the requirements of end-to-end encryption. These aspects are reflected in the investigation results. The WebRTC protocol is, according to the interviewed

---

[111] *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

[112] Cf. *IETF*, Messaging Layer Security: Secure and Usable End-to-End Encryption, available at: https://www.ietf.org/blog/mls-secure-and-usable-end-to-end-encryption/ as well as *golem*, IETF standardises Protocol for secure group chats, available at: https://www.golem.de/news/messaging-layer-security-ietf-standardisiert-protokoll-fuer-sichere-gruppenchats-2303-173089.html.

industry participants most frequently n used to encrypt audio and video telephony. The using services have also for the most part stated that they cannot encrypt video conferences in the group end-to-end.[113]

End-to-end encryption cannot currently be technically combined with certain **functions that** users like to use in video conferences: These functions include, for example, **dialling in from the public telephone network** or **the recording of meetings** by the service offering them. This is only possible if the service provider can access the data stream to include the audio call or record the data. The **connection of certain external devices** (e.g. room conferencing system devices based on the SIP protocol) is also not possible under end-to-end encryption, as this would require synchronisation of the different protocols. Leading services have explicitly pointed out just such restrictions and others, such as the **use of "assistants".**

Large video conferences for **webinars with several hundred participants** cannot currently be technically secured by E2E encryption. In this use case, it is necessary to check whether the service offering the service operates a video service location in Germany and whether this has been security-checked (for example, by a BSI C5 certificate).

Transport encryption and the secure operation of the video service in Germany should provide the

---

[113] In the past, a special interpretation of end-to-end encryption at a videoconferencing provider was noticed, which did not correspond to the actual definition of protection of data sent between the end devices of the users involved. The end point of the communication was not understood to be the users themselves, but the systems involved. In the case of videoconferences, these are often not the devices of the users, but the device of each user with the server of the service used. This corresponds to transport encryption. Due to the public criticism triggered by this in the press and the subsequent improvements also reported publicly, the Bundeskartellamt assumes that the answer to the questionnaire was based on the correct definition of end-to-end encryption, unless this can be concluded from the respondents' explanations anyway. See also, for example, *datenschutz notizen,* available at: https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597/ as well as *The Intercept,* Zoom meetings aren't end-to-end encrypted, despite misleading marketing, 31 March 2020, available at: https://theintercept.com/2020/03/31/zoom-meeting-encryption/ and *Golem*, Zoom advertises end-to-end encryption - which does not exist, cf. https://www.golem.de/news/homeoffice-neue-sicherheitsluecken-in-zoom-entdeckt-2004-147670-2.html.

criterion. Furthermore, it must be ensured that the identity of the participants can be established beyond doubt ("authentication"). End-to-end encryption ensures the integrity of the transmitted data. Without prior doubtless authentication, it ensures the protection of the transmitted data, but does not ensure who can receive this data.

b) Investigation results

On the question of whether and how encryption is used in the respective services, the Bundeskartellamt differentiated between text messages, telephone and video and distinguished whether users exchange information bilaterally or in a group. However, not all services offer full encryption of all functions mentioned by the Bundeskartellamt. End-to-end encryption is an option for many messenger and video services which can be set by the users (see section bb for details).

aa) Encryption of the functions

Overall view

When interpreting the results of the survey, it must be taken into account that some services do not offer all functions and that there are technical limitations in end-to-end encryption (see section D.I.4.a)cc) above). In addition, the various options that exist for encryption were implemented differently by the services in the questionnaire. For example, some respondents ticked everything including "no encryption", while others did not select any of the above categories and only used the option to enter a comment. The figures can therefore only be understood as a rough guide. According to their own information, 29 services use transport encryption for **text messages** both for bilateral exchange and in the group. End-to-end encryption is used by 22 services bilaterally and 19 for group exchanges. Both types of encryption combined are used by 16 services bilaterally and 13 in the group. For exchanges by **telephone,** 22 services use transport encryption for bilateral telephone calls, 18 also in the group. End-to-end encryption is used by 18 services for individual calls and 6 in the group. According to their own data, 12 services use both types of encryption for bilateral exchanges and 4 for group communication. For **video exchanges,** the number of services using transport and end-to-end encryption is slightly higher than for telephone calls. For bilateral video calls, 25 services use transport encryption and 21 services use end-to-end encryption. In the group, 22 services state that they use transport encryption. 11 services mention end-to-end encryption. Both types of encryption are used by 13 services, but partly only for bilateral video telephony.

	Text messages		Telephony		Video telephony	
	Bilateral	**Group**	**Bilateral**	**Group**	**Bilateral**	**Group**
Transport encryption	29	29	22	18	25	22
End-to-end encryption	22	19	18	6	21	11
Combined use	16	13	12	4	13	5

Figure 7: Type of encryption by function

Apart from **technical limitations,** various factors are cited as reasons why a certain function is not encrypted. These include user choice, availability only for business customers, in-house developments, browser requirements, compatibility problems or developments that have not yet been completed.

Video conferencing provider

Some leading video conferencing providers first explain how they **interpret** the **functions** mentioned by the Federal Cartel Office, as this is decisive for the implementation of end-to-end encryption. Basically, in the category "telephone", a distinction should be made between the audio channel of a meeting and the external dial-in to a meeting, e.g. via the public telephone network.
The situation was similar for the category "chat" or "text messages". Here, a distinction should be made between the exchange of text messages during a meeting ("meeting chat") and the chat function of the service, which may be independent.
In detail, however, there are differences in that not all functions are offered to every customer group or certain functions are defined company-specifically. Adobe clarifies that "telephone" is understood to mean the audio channel of a meeting and not the integratable telephone conference connection.
Google Meet explains that the chat function is linked to the video conference function. Users could only communicate with their fellow video conference participants.
-participants can send messages during the videoconference. Dial-up via the public telephone network would only be available to business customers, not to consumers using the free version.

Slack defines text messages as messages written within the Slack application between users. Telephony and video telephony would also be considered as
"messenger-internal" understood. No calls could be made to public phone numbers. Users could only connect with other Slack users in their team or other teams if their administrator allowed it.
Webex also explains the meaning of the "text" functions specified by the Federal Cartel Office, "telephone", "video". "Text" is interpreted as "online messaging", i.e. as a chat function. Telephone" refers to the "Webex Calling feature", which allows users to call colleagues within the company or contacts outside via the Webex platform.[114] "Video" corresponds to "Cisco's Webex online conferencing/meetings" offer, regardless of whether users call from the public telephone network or via VOIP, and regardless of whether they turn on their camera - exchange via video - or not.
Zoom also says that "text" refers to "meeting chat". Zoom's messaging function includes
actually two functions, the permanent chat ("Zoom Team Chat") and the chat during a meeting ("Meeting Chat"), which currently has to be actively saved as a text file if it is to be retained after the meeting. The participants in a video conference
could only exchange messages during the meeting via "Meeting Chat", not afterwards. The category "phone" corresponds to "Zoom Phone" ("Enterprise cloud phone system") and not to the dial-in to a Zoom meeting via the public telephone network. "Video" is interpreted as video conferencing in the sense of the content shared during a Zoom meeting or webinar.
The leading video conferencing providers make the following statements regarding the **encryption of their functions:**
Webex states that it uses **transport and end-to-end encryption for all types of exchanges offered.**
Since 2008, the clients' administrators have been able to activate full end-to-end encryption for video conferences (audio/video, 1:1 or in a group) on the software clients Mac OS, Windows, Android, Apple iOS. However, the basic technical limitations of end-to-end encryption apply. For new functions, including direct dialling in Webex teams (working groups), which do not currently support E2E encryption, the implementation of the MLS standard is under development, on the basis of which end-to-end encryption will be available to all conference participants.

[114] See Cisco, available at: https://www.cisco.com/c/en/us/solutions/collaboration/webex- calling/index.html.

functions can be applied. With its zero-trust approach, Webex offers both authentication and E2E encryption.
Zoom explains that end-to-end encryption can be set for "Meeting Chat". A corresponding upgrade is also available for some customers for bilateral telephone calls via "Zoom Phone". Phone calls in the group are not encrypted end-to-end. End-to-end encryption can be activated for video conferences.
With Skype, **bilateral exchanges** by phone, video and text message can be end-to-end encrypted, but not group exchanges.
Google Meet encrypts on the basis of the **TLS protocol**. All Google Cloud products, including Google Meet, are regularly subjected to an independent review of security, data protection and compliance. If the participants of a video meeting dial in by phone, the TLS protocol is of course not used. Adobe, Slack and Microsoft Teams also use transport encryption.

Free messengers and open source services

Element states that it can use end-to-end encryption for **all functions offered,** including group communication. Meet.jit.si also states that it can use end-to-end encryption for all functions offered, including group communication. The double ratchet protocol and DTLS-SRTP are used.
Jabber points out that the client software must support OMEMO encryption, otherwise text communication and file transfer is only TLS-encrypted. Transmitted files are temporarily stored on the server in OMEMO-encrypted form ("encryption at rest").
Telephony and video telephony use DTLS encryption. Blabber.im, Conversations, Dino, Quicksy can use end-to-end encryption for all their functions **except for group exchanges by phone or video.** They use WebRTC (DTLS-SRTP). Blabber.im explains it would use OMEMO or OpenPGP of the users' choice for text messages and AES 256 for file transfers in encrypted chats. DTLS-SRTP would be used for audio/video calls, TLS for transport encryption. Quicksy uses OMEMO and OpenPGP for text messages. For telephony, DTLS-SRTP is used and verified via OMEMO. Delta Chat explains that end-to-end encryption is possible because the service complies with the OpenPGP and Autocrypt standards for the exchange of text messages and files. Delta Chat has no influence on the encryption used for video telephony, but Jitsi, for example, is a WebRTC service.

More messengers

All the **services** they offer, **including group communication end-to-end encryption,** can, according to their own information, Ginlo, iMessage / FaceTime, Threema and WhatsApp.

Ginlo uses WebRTC, iMessage / FaceTime mentions SRTP. WhatsApp refers to its implementation based on the Signal protocol (Double Ratchet). According to Threema, group calls are currently in a beta phase, but are expected to be rolled out widely before the end of 2022. These audio and video calls in groups would be end-to-end encrypted. The encryption of Threema's content corresponds to the standard for audio and video calls between two people. Threema's communication is end-to-end encrypted and additionally transport encrypted with forward secrecy and key pinning[115] . For audio/video calls, WebRTC with SRTP and DTLS-SRTP 1.2 is used for key exchange. The session keys for DTLS are cryptographically bound to the end-to-end encryption of normal Threema messages.

Apart from group exchanges by phone or video, Line and also Viber use end-to-end encryption for their essential services - partly with restrictions. Line has implemented its own procedure for end-to-end encryption called "Line Letter Sealing". "Line

Letter sealing covers text messages (in bilateral chats and in group chats with up to 50 members), location messages (in bilateral chats and in group chats with up to 50 members), audio calls (1:1 calls) and video calls (1:1 calls). However, it is not currently applied to video and audio data sent as downloadable files (attachments). The details are - according to Line - publicly documented and available.[116] Viber, in turn, explains that its own protocol for end-to-end encryption uses the same concepts of the double ratchet protocol as used in the "Open Whisper Signal application". Nevertheless, Viber's implementation is new from scratch and does not use Signal's source code.

In addition, WebRTC would be used for audio/video communication.

[115] Key pinning is a mechanism to secure the HTTPS protocol against man-in-the-middle attacks with forged certificates signed by a recognised certificate authority, see e.g. *Wikipedia,* available at: https://de.wikipedia.org/wiki/HTTP_Public_Key_Pinning.

[116] Cf. *LINE Letter Sealing*, available at: https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver2.0.pdf.

Facebook Messenger uses transport encryption for text messages, and audio and Video calls (except "secret conversations")[117] are encrypted using SRTP[118] . In Facebook Messenger, content is mainly encrypted end-to-end in "secret conversations".

Some services mentioned **further or additional** (encryption) methods such as SRTP, RTSP[119] , AES[120] in relation to telephone and video communication and "full encryption"[121] .

bb) Activation of end-to-end encryption

Business customers who use the business solutions of the messenger and video services benefit from a wide range of settings that they can configure according to their needs.

---

[117] Technical Whitepaper, see *Facebook*, available at: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

[118] The Secure Real-Time Transport Protocol is the encrypted variant of the Real-Time Transport Protocol (RTP). The protocol was introduced by the Internet Engineering Task Force (IETF) in March 2004. It is particularly suitable for the encrypted transmission of communication via the Internet and is also increasingly used in IP telephony. The cryptosystem uses the Advanced Encryption Standard (AES). Depending on the implementation, the protocol can be used either for transport encryption during voice data transmission between an end device on the customer side and the server of the communication provider or for complete end-to-end encryption between communication partners, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Secure_Real-_Time_Transport_Protocol.

[119] The Real-Time Streaming Protocol (RTSP) is a network protocol for controlling the continuous transmission of audio-visual data (streams) or software over IP-based networks. It is used to control the session between receiver and server, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Real-Time_Streaming_Protocol.

[120] AES (Advanced Encryption Standard) is a symmetrical encryption method, i.e. the key for encryption and decryption is identical. The Rijndael algorithm has variable, independent block and key lengths of 128, 160, 192, 224 or 256 bits, see *Wikipedia*, available at https://de.wikipedia.org/wiki/Advanced_Encryption_Standard.

[121] The service defines this in such a way that all messages are encrypted not only during transport, but also on all participating end devices. The private keys for this are generated automatically by each user himself/herself by assigning a device password for each end device. Since these keys are only on the device of the respective user, neither the service nor a third party has access to them.

can make. Consumers, however, may not be aware of what options are available and what conditions they find in the applications they use. It may often be unclear whether end-to-end encryption is activated by default or whether it is an option that has to be activated, possibly for a **fee or if further conditions** are met. Therefore, the Bundeskartellamt has asked the messenger and video services to explain how end-to-end encryption can be activated and what the special features are.

Overall view

Of the services that use end-to-end encryption, 13 indicated that end-to-end encryption is **automatically and unchangeably activated** (BigBlueButton, Fastviewer, Ginlo, iMessage/ FaceTime, Loopup, Monal[122] , Nextcloud Talk, TeamViewer Meeting, Threema, Tixeo, Trillian, Viber, Webex, WhatsApp). For 8 services, the option is automatically activated, but for 6 of these services it can be changed by the users, for one service by the service itself and for two others by both users and the service itself.

For 10 services, end-to-end encryption is **not automatically activated**, but can be set by the user. One multi-messenger states that the range of functions is determined exclusively by the integrated third-party services.

In all groups of services, the **mechanisms** to **enable end-to-end encryption are** similar. Most services refer to the "Settings" to activate end-to-end encryption. Many services drew attention to the tapping of an icon. Meeting passwords and activation by an administrator are also mentioned.

Choice is particularly important with free messenger clients. With video conferencing providers, the respective administrator can often determine the level of encryption for the participants.

[122] According to the Messenger client, this applies from version 5.3.1. End-to-end encryption is then activated by default for 1:1 and group chats, provided these support this.
Users could still see in the chat window whether a communication was encrypted or not. Encryption could still be deactivated via the lock symbol and activated later. For technological reasons, public anonymous groups would not be encrypted end-to-end.

Video conferencing provider

With GotoMeeting, the password that protects the meeting must be entered. With Skype, "Private Conversation" must be selected to communicate end-to-end encrypted. Webex always uses encryption so that text messages, files, whiteboards and other content are only transmitted and stored in encrypted form once they leave the participant's device. Organisations can choose to use the cloud key management server (KMS) or operate a KMS themselves and thus manage the keys used in Webex themselves.

Companies can define different types of video conferences and their requirements for the type of E2E or transport encryption as "meeting templates" (templates with specific technical settings). The host can select from these templates the appropriate one for the planned meeting. For video conferences, the users can decide for themselves whether these should be encrypted. The administrator can also activate encryption for all or only some users or for all meetings. When planning the meeting, the host can also specify whether the standard level of security should apply or whether end-to-end encryption should be used (for example, according to the content of the discussion). Taking over key management requires establishing a comprehensive process for generating, securely storing and securely distributing keys. Loss or compromise of the master key is equivalent to loss or compromise of the complete data in the system.

Detailed instructions for account holders can be found at Zoom, and
Administrators in the "Help Centre" of the service.

Free Messenger /Open Source Services

With free messenger services, users can often decide for themselves whether and which encryption they use. The choice of server provider then determines whether and how encryption is used.

The free messenger client Delta Chat explains that encryption cannot be switched off completely, but users can choose to "rather not" encrypt. However, they would still reply to encrypted messages from others in encrypted form, as required by the https://autocrypt.org standard. With Dino, users have to select OpenPGP or OMEMO encryption for text messages/files; for telephony/video, end-to-end encryption is automatically activated, but without authentication/deniability if OMEMO encryption is not activated by users. At Gajim, end-to-end encryption is an easily accessible setting directly in the chat. At meet.jit.si, users can also find the setting in the meeting and chat options.

Security settings. For Monal, tap the lock symbol to deactivate end-to-end encryption for new versions of the messenger client and to activate it for older versions.[123] With Rocket.Chat, the key must be saved, which is created at the first login. In addition, the server administrator would have to make the corresponding setting.

More messengers

On Facebook Messenger, the content is mainly encrypted end-to-end in secret conversations. Users had to select "Secret Conversations" and activate the option of the same name by tapping on it.[124] This would be associated with various restrictions: "Secret Conversations" would only work with iOS and Android operating systems. Secret Conversations only allowed limited functions and could not currently be used as a group message. File sending (gifs), audio or video telephony and payments would also not be possible.[125]

Some messenger and video services are striving to improve or expand their encryption options. At Dino, end-to-end encryption with OMEMO will be activated by default in the long term, but users will be able to switch it off. At Monal, too, end-to-end encryption will be activated automatically in the future if long-term tests have shown sufficient stability. GotoWebinar states that LogMeIn is working on extended application possibilities for end-to-end encryption. Facebook Messenger (Meta) says it is working towards a global rollout of standard end-to-end encryption of personal messages and calls via Messenger in 2023.[126]

It is occasionally pointed out that end-to-end encryption in groups is being developed with the MLS standard.

---

[123] According to the Messenger client, E2E encryption has been activated by default for 1:1 and group chats since version 5.3.1, provided they support it.

[124] See *Facebook* 2017, Messenger secret conversations, Technical Whitepaper, available at: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

[125] See *Facebook*, Secret Conversations, available at: https://www.facebook.com/help/messenger-app/1084673321594605.

[126] See *Facebook*, Testing End-to-End Encrypted Backups and More on Messenger, available at: https://about.fb.com/news/2022/08/testing-end-to-end-encrypted-backups-and-more-on-messenger/

cc) Better encryption for a fee

In addition, the Bundeskartellamt asked the industry whether encryption against payment could be further improved. Here it emerged that the vast majority of services **do not** offer **additional encryption for a fee.** One service offers encryption of dormant data for business customers for a fee. Customers could also revoke encryption at various levels. Only one other service explained that it offered more extensive control over encryption procedures, but that end-to-end encryption was always included in the subscription regardless.

dd) Key management

Local whereabouts of the keys

Almost two thirds of the services stated that the **key is generated locally and the private key** remains **on the end device.**

Facebook Messenger explains that encryption is mainly used for "secret conversations" and that the cryptographic keys for this function are generated locally and remain on the end device. However, "secret conversations" would not be the only function for which cryptographic keys would be generated and stored locally within Facebook Messenger. Other functions such as transport encryption also generated such keys.

TeamViewer Meeting states that the keys for the end device and the private key are generated locally, whereby the private key can be extracted from the key of the end device for the purpose of password regeneration. Webex states that in transport-encrypted meetings, the servers generate the cryptographic keys and transfer them to the clients via TLS. With end-to-end encryption, the key is created by the host and passed on to the participants' clients. With the advanced version of end-to-end encryption that is being implemented - the Messaging Layer Security standard - the key is generated by each participant client based on the information exchanged via MLS. Companies can choose whether they want to use the cloud key management server or operate a KMS themselves and thus manage the keys used in Webex themselves. Zoom states that in end-to-end encrypted meetings, the key is created by the participants' devices, not by the Zoom servers. Encrypted content from customers cannot be read by Zoom because the necessary key is not available on the Zoom servers. In a meeting without end-to-end encryption, the keys would be created and managed by the Zoom servers.

Secure export and import

Eight services confirmed the **secure export and import of** the cryptographic key, albeit partly dependent on certain conditions, e.g. type of function.

Discord explains that for text messages, the asymmetric keys are generated locally and do not leave the device. The "server TLS keys" are managed by Cloudflare[127] . For audio and video exchange, a short-term key ("ephemeral encryption key") would be generated on the server and transferred to the clients for the calls. This key expires after the call and is not reused.[128] Facebook Messenger once again states that content is mainly stored at

"secret conversations" end-to-end encrypted. For "secret conversations", the cryptographic keys are generated locally and the private key remains on the end device.[129] Line explains that there is a "pairing protocol, which facilitates the transfer of private keys between two devices.

user clients via an "out-of-band channel". There is no general possibility to import or export private keys. Tixeo explains that no cryptographic keys are exported or imported. The Diffie-Hellman method is used. This does not use the secret

[127] Cloudflare, Inc. is a US company that provides a content delivery network, internet security services and distributed DNS services that reside between the visitor and the Cloudflare user's hosting provider and act as a reverse proxy for websites. A **Content Distribution Network** is a network of regionally distributed servers connected across the Internet to deliver content, especially large media files. A reverse proxy is a proxy in a computer network that fetches resources for an external client from one or more internal servers, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Cloudflare and *Cloudflare*, available at: https://www.cloudflare.com/de-de/.

[128] For more information on audio and video exchange, see *Discord*, available at: https://blog.discord.com/how-discord-handles-two-and-half-million-concurrent-voice-users-using-webrtc-ce01c3187429.

[129] More details about the key exchange are available from *Facebook*, available at: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

session key, but only the result of an arithmetic operation.[130] None of the services differentiated between operating systems. Two messenger and video services explained that the cryptographic keys were bound to the device account and stored in it. A new device would automatically receive new keys.

ee) Cryptographic principles

Overall, the property "Authentication" is used most frequently for messenger and video services, followed by "Perfect Forward Secrecy". "Deniability" and "Future/Backward Secrecy", on the other hand, are used less.

	Text messages		Telephony		Video telephony	
	Bilateral	**Group**	**Bilateral**	**Group**	**Bilateral**	**Group**
Authentication	27	25	21	15	24	18
Deniability	13	13	6	4	7	5
Perfect Forward Secrecy	19	17	12	7	17	14
Future/Backward Secrecy	11	9	6	3	8	5

Figure 8: Use of cryptographic principles by function

For the exchange in the group, the mentions are generally somewhat lower (see Figure 8).

[130] Diffie-Hellman key exchange is a method of securely agreeing a shared session key between two communication partners over a potentially insecure transmission medium. The secret key is never transmitted. The key is calculated via other transmitted information. For external attackers eavesdropping on the medium, calculating the shared session key is mathematically impossible with reasonable effort, see *Security Insider*, available at: https://www.security- insider.com/what-is-the-diffie-hellman-key-exchange-a-799443/. Diffie-Hellman is based on the "discrete logarithm" method. See on the "discrete logarithm" e.g. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch.

For bilateral **text messages**, 27 services apply "Authentication", 13 "Deniability", 19 "Perfect Forward Secrecy" and 11 "Future/Backward Secrecy". For communication in groups, the values are only slightly lower.

In the area of 1:1 **telephony**, just under half of the services mentioned "authentication". 12 from 44 services have specified "Perfect Forward Secrecy". 6 out of 44 services use "Deniability", as well as "Future Secrecy/Backward Secrecy". For groups, these percentages are significantly lower for all properties of the encryption methods.

For 1:1 **video communication,** slightly more than half of the respondents use "authentication". "Perfect Forward Secrecy" is cited by two fifths of the services. For "Deniability" and "Future Secrecy/Backward Secrecy", 7 out of 44 and 8 out of 44 messenger and video services respectively. For exchanges in group communication, the values in all categories are also lower here than for bilateral exchanges.

WhatsApp claims to implement all four characteristics in every type of exchange. The communication via Blabber.im, Dino, GotoMeeting, GotoWebinar, Viber, Webex is also characterised by the above-mentioned features to a high degree according to the responses of the services.

ff) Encryption of data on the terminal and storage encryption

13 messenger and video services state that they encrypt the data on the user's end device: Conferencing & Collaboration (for Windows), Element, Fastviewer, Ginlo, GotoWebinar, iMessage / FaceTime, Line, Skype (for "private conversations"), TeamViewer Meeting, Threema, Tixeo, Webex. The services that encrypt most frequently mention AES with 256 bit key length as the method. RSA, Cypher Suite[131] and SQL Cipher[132] are also mentioned.

Accordingly, isolated **differences** are described **depending on the user's operating system or end device in** the encryption procedures of the user's own messenger and video service. For example, a video conferencing service for the installed Mac client uses the system key to encrypt the data stored on the device. Under Windows, encryption is done with RSA. Mobile apps use SQLCipher, which provides AES 256-bit encryption of a local database. For a foreign service, full encryption on the device is only possible with desktop clients and browser extensions. A leading video service

[131] A cipher suite is a standardised collection of cryptographic procedures, for example for encryption, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Cipher_Suite.

[132] SQL Cipher is an open source software that provides transparent 256-bit AES encryption of database files, see GitHub, available at: https://github.com/sqlcipher.

explained that when his client is used, content is encrypted on the end device. If a web browser is used, content is not necessarily encrypted on the end device. The strength of the encryption and other details depend on the browser and also on the encryption methods agreed with the client.
Furthermore, different services point out differences depending on the **implemented client. The type of function used** can also determine whether encryption is used or not. For example, a video service popular with consumers uses encryption with AES only for "private conversations".

Another security aspect of messenger and video services in this context is whether there is **storage encryption.** Storage encryption (so-called data at rest) is aimed at data that is stored in some form on storage media. The message history on the end device and, if applicable, on backups can thus be protected from unwanted access and can only be read by the messenger app.

22 messenger and video services indicated that storage encryption exists. Services associated with operating system manufacturers and several free messengers and other services also point to the **possibilities of the operating systems** when it comes to encrypting data on the end device, such as storage encryption or device encryption for mobile operating systems or (hard disk) encryption for iOS and macOS. A free messenger client points out that the apps are also protected against data access on a mobile phone. As a rule, users are advised to encrypt their entire data and not just the messaging database.
BigBlueButton states that **no data is** stored on the end device. Meet.jit.si expresses a similar opinion. The only data stored on users' devices is the optional information about other meeting participants.

5. Further security measures

a) Two-factor authentication

aa) Background

When consumers use messenger and video services, they can ensure that third parties do not have unwanted access to their account and they themselves clearly

to which messenger and video services are **authenticated.**[133] This can be achieved with so-called two-factor authentication, provided it is available as an option in a system. With **two-factor authentication (2FA)**[134] or multi-factor authentication (MFA), not only a single personally chosen and fixed password or passphrase is used, but at least one additional authentication feature. It is important that the factors come from different categories. The first factor could, for example, come from the area of "knowledge" (e.g. password, PIN), the second from "possession" (e.g. chip card, TAN generator) or be based on biometrics (e.g. fingerprint, facial recognition).[135]

The additional factors usually have in common that they are created once and are only valid for a short time - a so-called **Time-based One-time Password (TOTP**) is generated. Once the password has been used or is not used within a certain period of time, it expires. Even if third parties know the actual password, they have only a few possibilities to also obtain the TOTP, or no time to find it out.[136]

---

[133] *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

[134] The BSI explains that the terms authentication and authentication are often used synonymously in common usage, but describe different sub-processes, e.g. of a login process. A user authenticates himself at a system by means of unique login information (e.g. password or smart card). The system then checks the validity of the data used, it authenticates the user, see *BSI*, available at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.

[135] Cf. *BSI*: Zwei-Faktor-Authentisierung - Mehr Sicherheit für Online-Konten und vernetzte Geräte, available at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.

[136] The Internet Engineering Task Force (IETF) published the Time-based One-time Password Algorithm in RFC 6238 in 2011 to provide more security on the Internet. See for example *IONOS SE*: Time-based One-time Password: TOTP explained, available at: https://www.ionos.de/digitalguide/server/sicherheit/totp/, *Twilio*: TOTP, available at: https://www.twilio.com/docs/glossary/totp, *Security Insider*: What is TOTP?, available at: https://www.security-insider.de/was-ist-totp-a-875708/.

The **process of** a 2FA transaction is usually that the user first enters their credentials to access the desired website or service. An authentication server checks the password. If it is correct, the user is qualified for the second factor. This is provided to the user by the authentication server as a unique code. By confirming the additional authentication, users confirm their identity.[137]

The second factor can reach the users in different ways: By email, by SMS or voice call, by biometrics-based 2FA, as one-click login / push notification, and as hardware token-based 2FA or via software token/ TOTP-based 2FA.[138]

For a long time, two-factor authentication via **SMS** was the most commonly used method. For this, the user leaves his or her own mobile phone number with the respective messenger and video service or other online service. If, for example, the user logs into a service on a PC with his or her own user name and password, the service sends an SMS with another code to the respective mobile phone. Users then enter this code on the website of the online service.[139] Less common is the procedure of sending the second factor **by e-mail** as a code or additional password. In any case, according to Stiftung Warentest, a different email account should be given than the one used for the login. Otherwise, an attacker who knows the password of the e-mail account can also intercept the one-time codes. Instead of looking at the

---

[137] See e.g. *IT Security Blog*: 2FA: Two-factor authentication with TOTP, available at: https://itsecblog.de/2fa-zwei-faktor-authentifizierung-mit-totp/.

[138] Cf. *Geekflare*: The 7 best two-factor authentication apps to protect your email and social media accounts, available at: https://geekflare.com/de/two-factor-authentication-apps/.

[139] Stiftung Warentest already pointed out in 2017 that the website usually only accepts the code within a short period of time. This further increases security. The procedure becomes even more secure if users use the settings of their smartphone to prevent it from displaying the SMS on the lock screen - and thus being visible to everyone. This can be prevented via the "settings" of the respective operating system, cf. *Stiftung Warentest*: So funk- tioniert Zwei-Faktor-Authentifizierung, available at: https://www.test.de/Online-Konten-schuetzen- mit-2FA-So-funktioniert-Zwei-Faktor-Authentifizierung-5177936-0/.

code, users of some services can also **call to** have the code sent to them.
leave it. The code is then announced by a computer voice.[140]
With **biometric systems, a** check is made when logging in to see whether one of the previously recorded unique physical characteristics (fingerprint, face, retina) is present on the user. As the BSI explains, biometric features are normally not "secret", so that life recognition is important so that the systems cannot be tricked with a photo, for example.[141]
The use of a **hardware token is** considered particularly secure and is being used more and more. A personal USB device ("token") is used as a second identification factor. This is a special USB stick on which a digital security key is programmed. For initialisation, users insert this stick into the USB port of their computer. After entering their user name and password on the website of the service they are using, they press a button on this stick when prompted, whereupon the process is released.
When services use "**one-click login**" or "**push notifications**", users do not have to enter a second code. Instead, a message appears on the smartphone that the user has to confirm. These so-called push notifications are messages that appear on the smartphone without opening the respective app.
Finally, the time-based one-time passwords can also be generated in an **authentication app** every few seconds. To do this, users must install a free TOTP app on their smartphone once. The desired app can be downloaded from the smartphone's app store. Then the security settings of the website or service that the user wants to use with a 2FA must be opened on the computer. Then the 2FA can be selected and activated. The QR code displayed for setting up the 2FA must be scanned with the app. The authentication app is then connected to the

[140] Cf. *Stiftung Warentest*, available at: https://www.test.de/Online-Konten-schuetzen-mit-2FA-So-funktioniert-Zwei-Faktor-Authentifizierung-5177936-0/.

[141] Cf. *BSI*, Zwei-Faktor-Authentisierung - Mehr Sicherheit für Online-Konten und vernetzte Geräte, available at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.

service and generates a new unique code every thirty seconds.[142] Users can also use the authentication app without a mobile network or internet connection.

bb) Investigation results

Half of the messenger and video services indicated that they offer proof of identity through a combination of two different and, in particular, independent factors. Two-factor authentication should be an option that users can set (e.g. Discord, Element, Facebook Messenger, Google Meet, GotoMeeting, GotoWebinar, Nextcloud Talk, Rocket.Chat, Skype, Slack, Snapchat, Microsoft Teams, TeamViewer Meeting, Threema, Trillian, Webex, WhatsApp, Zoom). Google states that in future it will no longer just recommend 2FA, but want to integrate it automatically.[143] For some messenger and video services, 2FA is only possible or preset for business customers (e.g. Trillian or Microsoft Teams).
A multi-messenger explains that whether 2FA is offered depends on the service. Meet.jit.si points out that since there are no accounts with Jitsi, there is no authentication. The industry as a whole uses a number of methods, of which the services then individually implement a certain selection. Some large services offer users **different options for 2FA.** With a large "Platform", users must also enter a code from their time-based one-time password (TOTP) authenticator app, a backup code or a one-time code sent to them by SMS when they enter their password to log in. Even with a leading messenger service, users can choose between three security methods for two-factor authentication: Either they enter an additional

[142] See e.g. *datamate*: The seven best 2FA apps for Android and iOS, available at: https://www.datamate.org/die-7-besten-2fa-apps-fuer-android-und-ios/, *Web.de* Blog: "OTP app" - what is it?, available at: https://web.de/email/tipps/posts/was-ist-eine-otp-app/286/, *pcvisit*: Two-factor authentication: These are the best apps, available at: https://www.pcvisit.de/blog/2020/07/23/zwei-faktor-authentifizierung-das-sind-die-besten-apps/.

[143] In May 2021, Google, Apple and Microsoft announced they would extend support for a common passwordless login standard developed by the FIDO Alliance and the World Wide Web Consortium, see Apple Newsroom, available at: https://www.apple.com/de/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded- support-for-fido-standard/.

security code on a compatible device, or they use login codes from a third-party authentication app, or they have a code sent to them via SMS. The service of a large digital company also explains that its service has different procedures, including

Security key, authenticator and "SMS text message". A well-known video service mentions as an option to use "authentication apps" that support TOTP such as Google Authenticator, Microsoft Authenticator, and FreeOTP. Users could alternatively have the service send them a code via SMS or phone call as a second factor in the authentication process. Two other services also mention TOTP Authenticator Apps or the security SMS or email.

Furthermore, TOTP as well as 2FA devices are also referred to. One service that advertises high security uses a device password plus private key. In another such service, the email address and/or mobile phone number can be linked and the code sent by email or SMS.

A popular service among consumers allows users to enter an email address and use a "two-step verification code".

Some services refer to the **service providers or "identity providers**" that offer 2FA, MFA and single sign-on. A leading video service explains that customers' administrators can activate their own multi-factor authentication (MFA), which runs with OTP (one time password) solutions such as Duo, Microsoft Hello or Google Authenticator.[144] This

"Identity providers would offer MFA for user authentication. Alternatively, single sign-on could be set up[145] . For another video service, users can also introduce single sign-on (SSO) with two-factor authentication.[146] For authentication

---

[144] See *Webex*, available at: https://help.webex.com/en-us/52szeq/Enable-Multi-Factor-Authentication-Integration-in-Webex-Control-Hub.

[145] See *Oasis*, available at: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf.

[146] With single sign-on (SSO), a user can access all computers and services for which he or she is locally authorised from the same workstation after a one-time authentication at a workstation, without having to log in to the individual services each time. If the user changes workstations, the authentication, as well as the local authorisation, becomes invalid, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Single_Sign-on.

Twilio[147] can also be used as a 2FA provider. Two other video services also refer to "Third-party identity providers, including Azure AD[148] , Okta[149] , and OneLogin[150] , which provide two-factor authentication and to which users of the service can connect.

For messenger and video services linked to the manufacturers of the major operating systems, 2FA is linked to a corresponding **account** (Skype, Teams, Google Meet). Users who want to use Facebook Messenger must be registered with Facebook anyway.

[147] Twilio is a US company that operates a cloud communications platform as a service. It is based in San Francisco. Twilio enables software developers and companies to make and receive calls, send and receive text messages and perform other communication functions programmatically using a web service programming interface, see *Wikipedia*, https://de.wikipedia.org/wiki/Twilio or *Twilio*, https://www.twilio.com/de/.

[148] Azure Active Directory is a cloud-based service from Microsoft for managing identities and access rights, cf. *Cloudcomputing Insider*, available at: https://www.cloudcomputing- insider.de/what-is-azure-active-directory-azure-ad-a-946693/. The enterprise identity service *Azure Active Directory* (Azure AD) offers single sign-on (SSO) and multi-factor authentication, see https://azure.microsoft.com/de-de/services/active-directory/.

[149] Okta, Inc. is a publicly traded identity and access management company based in San Francisco. It provides cloud software that helps organisations manage and secure user authentication in applications and enables developers to integrate identity controls into applications, website web services and devices. Okta markets six services, including a single sign-on service that allows users to log in to a variety of systems through a centralised process. It also offers API authentication services. Okta's services are based on the Amazon Web Services Cloud, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Okta_Inc. or *Okta Inc.*, available at: https://www.okta.com/de/.

[150] OneLogin, Inc. is a cloud-based identity and access management provider that designs, develops and sells a unified access management platform for enterprise-level businesses and organisations, see *Wikipedia*, available at: https://en.wikipedia.org/wiki/OneLogin or *OneLogin* available at: https://www.onelogin.com/de.

b) Security copy (backup)

aa) Background

Finally, the messenger and video services had to indicate whether users can create a backup of their data. A backup refers to a copy of existing data on another medium to protect against data loss due to hardware failures, software problems, natural disasters or external threats such as malware. The backup copy can be created on an external hard drive, the computer's hard drive or even on a USB stick. The data can also be backed up online.[151]

bb) Investigation results

Two thirds of the services indicated that they have such a function. These include Adobe, Blabber.im, Conversations, Delta Chat, Dino, Discord, Element, Facebook Messenger, Gajim, Ginlo, GotoMeeting, GotoWebinar, IMessage/FaceTime, Meet.jit.si, Line, Quicksy, Rocket.Chat, Skype, Snapchat, Teams, Threema, Tixeo, Trillian, Viber, Webex, WhatsApp, Zoom.
For some services, the possibilities are linked to various requirements or to certain functions. For one service, the possibility of exporting a chat history only exists for logged-in users with appropriate permissions in the room (organiser role). The possibility to create a recording of the audio/video tracks in the room requires the same permissions. This is not a backup in the strict sense. It is also stated that it is not possible to back up the chat history, but users can record calls during the conference. A well-known video service distinguishes in this context between its own chat function and meeting chat, the chat during a meeting. With the chat function, a backup could be made, but with meeting chat this was only possible under certain conditions, e.g. if a meeting was recorded or the chat was saved as a text file, provided this had been activated by the administrator.
With an open-source client, users can hold their video meetings in their own
Save "Dropbox accounts". A popular service offers end-to-end encrypted backups.

---

[151] Cf. e.g. For example, Storage-Insider, available at: https://www.storage-insider.de/was-ist-ein-backup-eine- datensicherung-a-621411/ or *CHIP*, available at: https://praxistipps.chip.de/was-ist-ein-backup-einfach-erklaert_41415.

II. Data processing

Part of the Bundeskartellamt's investigation was focused on the data processing of messenger and video services. This involves how and why data is collected, where it is stored, to whom it is passed on, whether and when it is deleted, and (for selected questions) whether practices of the services comply with the legal requirements - the European GDPR.

1. Registration

a) Background

When registering, most messenger and video services ask consumers to provide personal data. However, the extent to which data is disclosed can vary widely. In the case of applications for business customers, the variety of choices during registration reflects customer wishes, which can thus be implemented in a company-specific manner.
The Bundeskartellamt asked the messenger and video services which minimum requirements must be met in order to be able to use their messenger/video service for exchanges by text message, telephone or video (in each case 1:1 and group) in Germany as an administrator/host or as a participant (see b)aa)). Possible requirements were the provision of an email address, the click on a confirmation email, the provision of a name, a telephone number, the assignment of an ID by the provider, the assignment of a password and the agreement to the privacy policy, the terms of use and the general terms and conditions. In addition, other requirements could be specified. If necessary, the information was to be explained. A distinction had to be made between the roles of "host/administrator" and "participant" (see b) bb)).

b) Investigation results

aa) Registration requirements

<u>Overall view</u>

Individual messenger and video services state that registration applies to all functions and services. The differences between the registration requirements for exchanges via text messaging, telephony or video telephony are not significant according to the findings, even if the requirements for exchanges via video are slightly higher on average. For both text messaging and telephony and videotelephony exchanges, the
Registration requirements for the role of "host" slightly higher on average than for participation.

On average, messenger and video services most frequently require **an ID and a password** for registration**, as well as agreement to the privacy policy, terms of use and general terms and conditions**. This is followed by an email address and then a name.

Free Messenger / Open Source

For the use of XMPP, the assignment of an ID and a password are obligatory. Data protection declarations, terms of use and general terms and conditions are usually publicly documented by server providers and confirmed via a web form when the account is created. The same applies to messaging via the e-mail architecture.

In this context, the free messenger clients explain the separation between application and system or service provider. Three XMPP clients make it clear that a client can be used with any XMPP services (servers) (similar to email). Users could use any XMPP server with which they set up an account. All the requirements in the Bundeskartellamt's question varied depending on which "service provider", e.g. server operator, consumers chose. These set different requirements, which could include, for example, agreeing to T&Cs and providing an email address. Another XMPP client agrees that the use of public or private XMPP services of third parties, e.g. server operators, may require the provision of personal data or consent to terms of use. However, this is not strictly necessary to use the client, especially if the user is a service provider.

email client Delta Chat explained that users could use any email address to send and receive messages. Neither the operator "Merlinux GmbH" nor any actor or actor associated with it received knowledge of this email address, let alone passwords or messages. This is due to the strict separation of apps and message transport, a long-established practice in the e-mail system. The Delta Chat project and the offers in the app stores showed that this could be achieved without any major loss of usability and quality.

"Convenience" is possible. In Delta Chat, (video) telephony is realised through the integration of Jitsi instances. The users can choose a Jitsi instance on which a room is to be opened. No personal data is transmitted to Jitsi. In addition to Jitsi, other services such as BigBlueButton could also be used. merlinux GmbH does not have any knowledge of these uses either, as communication only takes place between the installed app and the video servers, into which Delta Chat generally has no insight, not even an encrypted one.

Rocket.Chat argues similarly to the free messenger clients. The service is open source and highly adaptable to the needs of users. All types of

Registration may be required, but this is the decision of the respective server administrator and is not prescribed by the service itself. Especially for exchanges by telephone and video, it depends on which service is used.

The Matrix client element requires users to have an ID and password and to agree to the privacy policy, terms of use and T&Cs. For text messages, an email address is also required with a click on a confirmation email.

The open source video conferencing application Jitsi Meet does not require user accounts to be created and registration data to be entered. In the case of the application meet.jit.si. questioned by the Bundeskartellamt, the operator "8×8" collects network and user information including the IP addresses of the participants in a meeting, the specific URL through which the meeting is hosted and, if applicable, information about the telephone numbers that dial into the meeting (if the audio connection is made via telephone dial-in).[152] BigBlueButton (BBB) is also open source software, especially for online learning and audio/video conferencing. Based on BBB, there are different operators with different business models that determine the individual configuration and registration requirements.

Other messenger and video services

With many well-known services, an **account** must be created during registration. With Discord, users have to create a user name and password and provide either an email address or telephone number. This applies at least if they want to log in and out or if they want to use the service on different devices. Otherwise, they could initially also log in with a user name and their date of birth. Those who want to use Facebook Messenger must first create a Facebook account. For this, the name, either an e-mail address or a mobile phone number, password, date of birth, gender must be entered. The email address or mobile phone number must be confirmed.

Users could use the messenger even if they had deactivated their Facebook account. Participants only do not have to identify themselves with name and password if the "Guest Chat mode" is set in the "Chat Plugin", which is hosted by a third party website.[153]

With Snapchat, too, either the email address or the telephone number must be entered for the creation of an account, as well as the name, password and date of birth (because of the

[152] Cf. *meet.jit.si* Privacy Supplement, available at: https://jitsi.org/meet-jit-si-privacy/.

[153] See *Meta for Developers*, available at: https://developers.facebook.com/docs/messenger-platform/discovery/facebook-chat-plugin.

age rating), and consent to the terms of use and privacy policy is also required. Snapchat does not distinguish between "administrators/hosts" and participants.
How other services deal with this distinction and what implications this has for data collection will be briefly described in the next chapter.

bb) The roles of "host" and "participant

For the sector enquiry, the Bundeskartellamt distinguished between the functions of a host (also organiser, administrator) and a participant. According to this, host was used as a collective term for a person or institution that can actively start an exchange via text messages, telephony or video telephony and invite other participants to it and, if necessary, has further authorisations (e.g. muting participants, deleting groups, removing participants, etc.).
In contrast, participant refers to any person or institution that merely responds to
"Invite" a host to participate in an exchange via text messaging, telephony or video telephony (individually or in groups).
Consumers are probably most familiar with the distinction between "host" or "participant" from **video conferencing providers**, which have been part of everyday life for many at least since the beginning of the pandemic. Almost all of the messenger and video services that
responded provided information on both the "host" and "participant" roles. Among videoconferencing providers, there are some commonalities in the definition of these roles, but also many differences and configuration options from which customers can choose. In principle, more registration data is required for the **role of "host/administrator"** than for participants. However, the hosts themselves can often determine which data the participants have to register with. This may require the **creation of an account** with the corresponding data entries.
At GotoMeeting, administrators/hosts need such an account to use the service and start audio and video conferences and chat. Registration for this requires name, email address, password and a user ID, as well as agreement to LogMeIn's Terms of Service and Privacy Policy, both of which are available online. However, participants in a meeting started by a host do not have to register. Providing a name or email address is then optional. With Webex, too, participants in a video conference - unlike the host - do not have to register with an email address and password. It is not necessary to enter a name with Webex. However, an administrator of a corporate client can set many things, e.g. that all users must enter their first and last names.

last name would have to be entered. In the case of video conferences with several parties via Webex, the participants would have to enter an email address, but its validity would not be checked, the typical format of an email address would suffice. There would be no verification based on this email address. User account created. Microsoft Teams also explains that as an "unauthenticated guest" no valid email address or name has to be entered. Only the terms of use, including the privacy policy, have to be agreed to. According to Teams, the registration requirements for business versions of Teams are otherwise identical for hosts and participants, namely email address, name, ID, password and agreement to the terms of use, privacy policy and TOS.[154]

The registration requirements for the open source offering Nextcloud Talk also differ depending on the role. Nextcloud Talk does not offer its own service. Customers operate Nextcloud (Talk) on their servers themselves. Every person who has a user account on the Nextcloud instance with Nextcloud Talk can use Nextcloud Talk as a host depending on the configuration. After the initial creation of a user account on Nextcloud, no further data would be required to conduct video conferences, chats or telephone calls. No data is required as a participant, even the name does not have to be entered (the default is simply "guest", if not defined otherwise).

Even if users make use of the **free offer of** a video service, an **account** must be created for this purpose with some services, the registration requirements of which largely correspond to those of a business offer. This is the case with Google Meet, for example. Google Meet explains that consumers who want to use the free version must first create a Google account in order to access Google Meet. This was independent of whether they saw themselves as a "host" or "participant". To do this, an email address, name, ID and password would have to be entered. In addition, consent to the privacy policy, terms of use and general terms and conditions is required. If users already had an account, there were no additional registration requirements to use Google Meet. With the business offer, however, registered "hosts" could invite participants who did not have a Google account, e.g. for a cross-company video meeting.

[154] Microsoft Teams points out that the answers in the questionnaire refer to the business versions of Teams, which are offered as part of Microsoft 365 and Office 365. Although a consumer version of Teams would also be available in the meantime, this would only have been the case after the deadline for answering the questionnaire.

As participants in a **free offer, functional limitations must** be expected in comparison to the paid offer. Zoom, for example, stated that the questionnaire was answered from the perspective of users who wanted to use the free offer and act as host/administrator. As a host on the basis of the free version, name, email address, click on confirmation email, date of birth and a password must be entered as well as agreeing to the data protection statement and the
Terms of use had to be agreed to. Furthermore, the category "participants" was filled in from the perspective of users who had been invited to meetings by hosts/administrators but who had not registered. Participants would only have to agree to the privacy policy and terms of use. These users could only use the chat during a meeting, not Zoom's own chat function.
If video services are aimed **exclusively at consumers**, this does not necessarily mean that the registration requirements are lower than for services aimed mainly at corporate customers, especially if an account has to be created. Skype, for example, is described by Microsoft as a "consumer communication service". Users have to enter their e-mail address, name, ID and password. There is no differentiation between administrators/hosts or participants. Snapchat also does not distinguish between administrators and participants after an account has been created.

Other messenger and video services

The well-known messenger and video services that are particularly popular with consumers do not distinguish between administrators and participants. This applies, for example, to Discord, iMessage / FaceTime, Snapchat, Threema, Viber and WhatsApp. The requirements are also the same for Facebook Messenger as far as the information to be provided in order to be an administrator or participant is concerned. For participants of the video function, less data information is required, unless administrators set additional requirements.

Free Messenger / Open Source Services

In the case of free messaging systems and open source applications, the distinction between administrators/hosts and participants is not intended in principle, but ultimately depends on the design by the respective (server) operator. For example, the BigBlueButton application "vicole", which was questioned by the Federal Cartel Office, also requires administrators to

Administrators have to enter their e-mail address, click on the confirmation e-mail, enter their password and agree to the general terms and conditions, terms of use and privacy policy, while participants only have to enter their name. With Delta Chat as a free messenger client, there is no distinction due to the "email architecture".

2. Dealing with contacts

a) Background

The question of how a messenger and video service handles users' **contacts**, i.e. whether the user's contact directory or address book is accessed, is less relevant to services that deal with video conferencing, especially in the business customer segment. Customers conduct videoconferences within a defined circle of participants. Ensuring confidentiality and discretion of the information shared there is an essential part of the business model of these video conferencing providers. Often the client's administrator can determine what registration requirements are imposed on participants.
This can be different for services with a focus on messaging for consumers, especially for free services. Not only the telephone numbers of the users themselves, but also the telephone numbers from their address books are then uploaded to the server and, if necessary, displayed (contact discovery). In this way, telephone numbers of users who are not registered with the respective service and have not consented to the general terms and conditions can also reach the servers of the services.
A privacy-oriented messenger and video service has stated that especially with the concrete
There are "huge differences" in the implementation of synchronisation as far as privacy is concerned, which should be taken into account in this consideration. These include not only the type of information (data) that is transmitted, but also whether it is encrypted, whether the data can be read by the operator and whether it is stored by the operator.
Not only for consumers themselves, but also for an evaluation of messenger and video services in terms of data protection law, the question of how data is handled, in particular the identity of users and their contacts, is particularly important. The Bundeskartellamt has therefore requested information on which requirements users must fulfil in order to be able to use the respective service.

b) Investigation results

Five messenger and video services that do not focus on video conferencing require **a phone number to be entered for** the exchange, as a participant or as a host. Two services require a phone number only for the host function. Otherwise, the telephone number is not mandatory for messenger and video services that focus on video conferencing. In the case of a video service, for example, a telephone number is only required if users wish to exchange information as participants or hosts by telephone.
With regard to data processing when **synchronising the contact directory,** almost a third of the messenger and video services initially indicated that they carry out such synchronisation; these were predominantly internationally active services with large numbers of users. The users apparently consent in a similar way: they select the optional feature or agree on a specific **button of the app that** data is collected and passed on, or they select the corresponding option in the **settings of** their end device. In the case of Facebook Messenger, the synchronisation of contacts must be permitted both via a button in the settings and separately in the settings of the respective end device.
Individual services that belong to strong market, globally active groups have emphasised that users must actively synchronise the contact directory. In this context, Threema also emphasises that **synchronisation is completely optional**. Since Threema is not based on mobile phone numbers as identifiers, there are no functional restrictions.
Threema points out that in the context of this Contact Discovery, only the "minimal information" would be transmitted, these would be encrypted and not readable by the operator. It would only be held briefly in the working memory and not stored. Zoom also states that it does not synchronise by default, but only offers a synchronisation option.
In contrast, three free messenger clients explicitly pointed out that they do not synchronise the contact directory.
A lack of consent to processing does not make it impossible for users to use the service in any of the other services concerned. It can only result in certain restrictions. For example, some services pointed out that if the user
"Friends" cannot be found or only limited contact suggestions are made. The majority of the services surveyed do not synchronise the contact directory according to the results of the investigation.

3. Storage location of the data

Less than a third of the services store at least one category of data within the EU - i.e. within the scope of the GDPR. Specifically, the data is stored primarily in Germany, but also in France or the Netherlands. This suggests that a clear majority of services store their data outside the EU.
Seven services explicitly stated that they store at least one category of data only in the US. A quarter of respondents on average indicated storing one category of data in a public cloud - mostly by one of the technology companies Google (Alphabet), Amazon, Apple or Microsoft. Free messenger clients have indicated that the location of data storage depends on the users' choice of server. Some services maintain storage infrastructures in the EU and in third countries, especially the USA. In some cases, it remained unclear where EU citizens' data was transferred to. In part, this was dependent on various constellations.

4. Further investigation results

As part of the investigations, the Bundeskartellamt also questioned the messenger and video services about other aspects of data processing. The topics of the questioning were in particular the collection, purpose of storage, transfer and deletion of individual categories of data, consent to data processing, revocation options, functional restrictions in the absence of consent as well as informing users about data processing. Several services have explicitly indicated in the general comments on this topic that they consider their approach to data protection to be compatible with the requirements of the GDPR.
For the various questions on the scope and type of data processing, the Bundeskartellamt had specified and defined seven different data categories in the questionnaire (Figure 9):

The questions were answered plausibly and evaluably by a total of 36 services. Some free messenger clients and one multimessenger did not provide any detailed information here, but

➔ **Personal data:**

First or last name of the user, user name or pseudonym (e.g. alias/nickname), date of birth, age, gender, nationality, email address, telephone number, postal address, account information, private key for encryption.

➔ **Unit / configuration data:**

IP address, operating system, network operator, device type, device IDS, IMEI (15-digit serial number for smartphones), user accounts, passwords, fingerprint, certificates, installed apps, region and language settings

➔ **Location / movement data:**

Whereabouts, time of stay, duration of stay, movement profiles

➔ **Contacts / third party data:**

Contact directory, address books

➔ **Group memberships:**

Participant or organiser (host) in chat groups, telephone conferences, video conferences

➔ **Usage behaviour:**

Frequency and Durati the Messenger app use, Online/offline status, Browsing history/browsing chronicle, use of different end devices, type of devices, times / duration / Participants in an exchange via text message / telephone call / video call (in each case 1:1 or in groups)

Figure 9: Data categories

pointed out that the decision on data collection/processing does not lie with them, but with the respective server operator or integrated third party services. Most messenger and video services have also stated that their data processing policies apply equally to text, phone and video exchanges, whether bilateral or in a group. Some services that differ in this regard have explained that video or phone conversations (unlike text messages) are not stored retrospectively.

a) Reason for and purposes of data collection

Occasion

The Bundeskartellamt asked the services whether they collect data from the categories mentioned when registering, using or synchronising the contact directory. Figure 10 below shows how many services indicated that they collect data from the respective category during the various actions:

Almost all services stated that they collect personal data from users during **registration**, and half of the services then also collect device or configuration data. None of the services already collect users' contacts during registration. Some services indicated that they do not require registration (e.g. as an invited participant in a video conference) and therefore no data can be collected during this action. When using messenger or video services, significantly more services collect data than when simply registering. According to the survey, most services receive personal data, device/configuration data, group memberships, usage behaviour and content. Some services also collect location/movement data or third-party contacts/data during use.

With regard to the **synchronisation of the contact directory,** the services surveyed answered much more cautiously. Almost a third of the messenger and video services stated here that they collect the contacts of the users or the data of third parties (see D.II.2.b) for the results of the investigation). Only in isolated cases do the services also receive other data.

Individual services have also referred to the **collection of further data** at this point. These include the duration and the number of participants in a call, the possibility of the

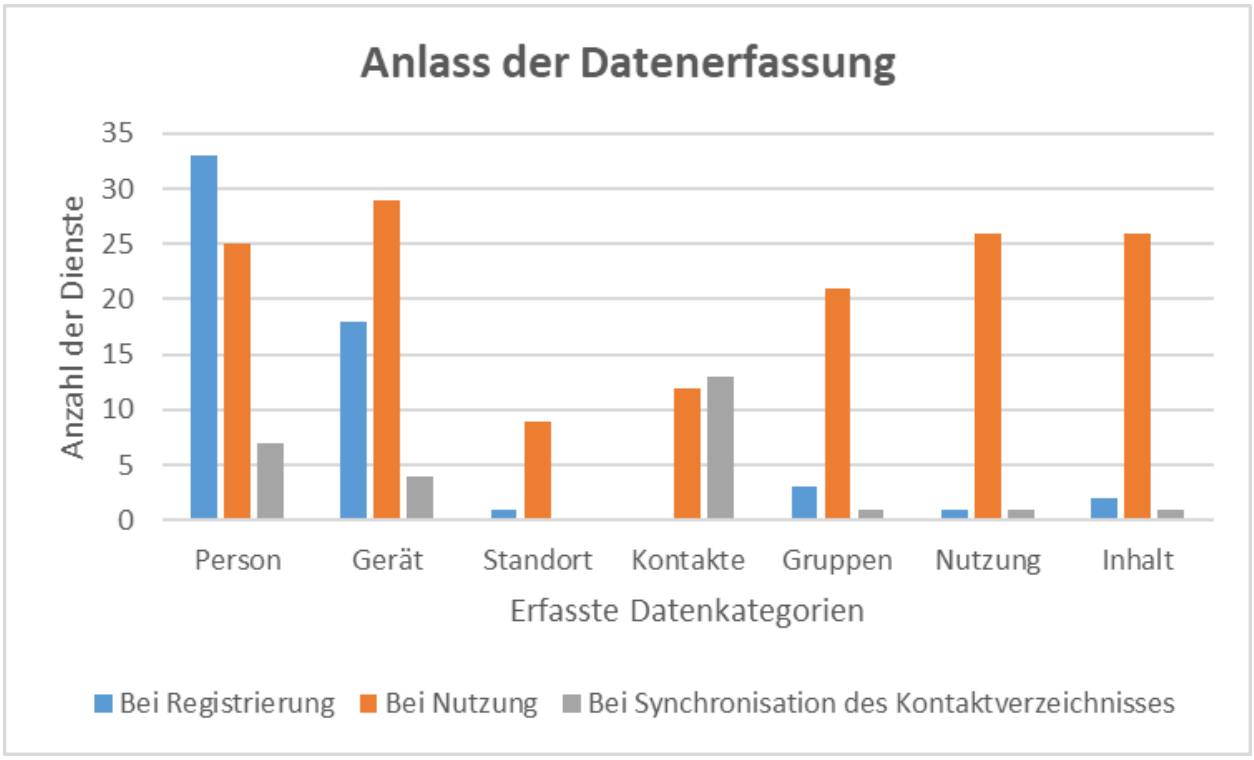


Figure 10: Reason for data collection

location sharing with other users and the recording of the location in the event of an emergency call.

Purpose

Another block of questions concerned the purpose of data collection. The messenger and video services were each asked to answer to what extent they collect the individual data categories for functionality, for their own advertising purposes or for passing on to third parties. The following figure 11 shows the distribution of the answers:

Almost all of the messenger and video services have stated that they collect personal and device/configuration data for the **functionality of the service.** More than half of the services also mentioned this for the data categories "usage behaviour", "group memberships, contacts/third party data" and "content". Only about one third of the services collect location/movement data of users for the functionality of the service, according to the survey results. These included the popular services Skype, Snapchat and Microsoft Teams. The reasons given for collecting data included the performance and reliability of their own messenger and video service or its improvement, as well as checking spam filters or improving interaction with users.

Significantly fewer respondents collect data **for their own advertising purposes**. Examples of own advertising purposes included service recommendations via email, an online sticker shop and

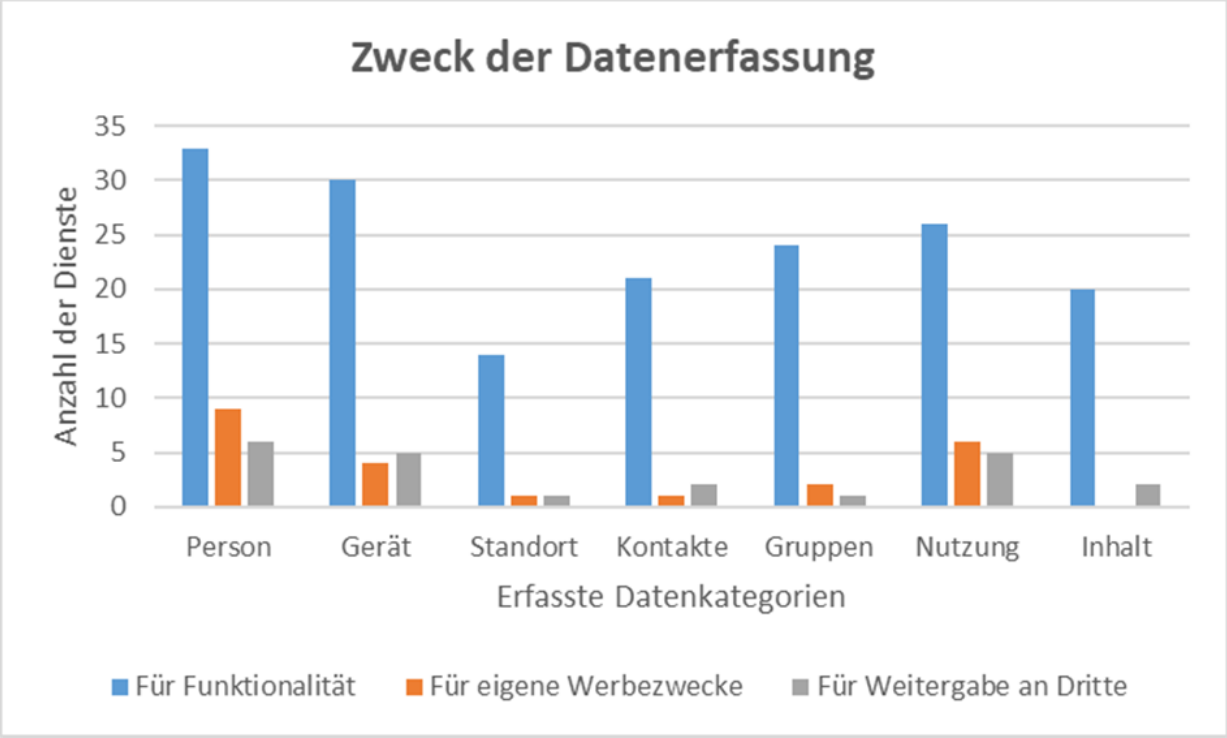


Figure 11: Purpose of data collection

personalised product recommendations and marketing purposes. Only individual services stated that they use personal data, usage data and device/configuration data for this purpose. Only one and two services respectively stated this for the data categories "group memberships", "location/

Movement data" or" Third party contacts/data". No service indicated in the survey,
capture content for their own promotional purposes.
A similar picture emerged when asked which data categories the messenger and video services register in order to **pass** them **on to third parties**. A small proportion of the services pass on personal data, device/configuration data or data on usage behaviour to third parties; the other data categories were only mentioned by one or two services. Individual services explained that they may pass on data to law enforcement agencies. Some of the interviewed video
Services provide the collected data to subcontracted processors, according to their own statement. ("subprocessors") are ready.

b) Disclosure and deletion of data

According to the results of the investigation, significantly less than half of the messenger and video services pass on and process individual categories of data **internally.** The services in question justified this in particular by wanting to improve marketing, security and performance or to ensure disclosure to authorities. Three popular services with high user numbers explained that employees within the group have access to the data under certain conditions, even if no explicit disclosure of the data takes place.
The answers regarding the passing on of data **to third parties** were clearly different: Only one service in each case stated in the survey that it passed on personal data or device/configuration data to third parties.
Facebook (now operating under the name "Meta"), partly with reference to the explicit consent of the users. Data transfer to Google was confirmed by a few individual services for each of the seven data categories, with a slight focus on the categories of device and configuration data and user behaviour. Some messenger and video services explicitly mentioned the use of the "Google Cloud" and "Google Analytics". A few individual services also stated that they pass on device and configuration data, data on user behaviour or personal data and content to external data analysts. The analysis of service quality was mentioned here as an explanation, namely the analyst "Amplitude".
Otherwise, individual services transfer data to subcontractors, law enforcement agencies or business partners; thereafter, personal data, device information and user behaviour data are sometimes passed on.
The Bundeskartellamt also requested information on the **deletion of data.** In particular, for the data categories "device information" and "usage behaviour", several messenger and video services have indicated that these are deleted in a period of 0 to 12 months. However, some services explained that the time of deletion varies depending on the type of data. For example, data from private customers is sometimes deleted earlier than data from

Business customers. Video recordings or voice messages are deleted sooner than other content, and stored movement/location data is also subject to shorter periods of time before deletion. Several services stated that (automatic) deletion of data happens after the end of the contract or after deletion of the account. However, some services also emphasise that the data is deleted at the request of the user.

On the question of the conditions under which it is possible to delete a user account, the respondents expressed very different opinions. For two open source services, no account can be deleted because no data is stored or no account is created. For some services, the administrators and server operators have to implement the deletion; for others, the users can do this themselves.

c) Consent to data processing

On the question of the **reason for and form of consent to** data processing, several mainly large messenger and video services explicitly stated that users actively consent to data processing during registration. However, the specific form in which this consent takes place was only partially explained. Some services pointed out that they do not require registration at all. Some other services also stated that users must consent to data processing vis-à-vis third parties (e.g. the server administrator).

On the question of how users can **revoke** their consent to data processing, the messenger and video services surveyed provided very different information. Among other things, some services mentioned the possibility of direct contact, revocation through corresponding settings in the declaration of consent or switching off the corresponding setting, as well as revocation through deletion of the account. Individual services also indicated that revocation was not possible or only possible to a limited extent, as otherwise the functionality of the service could no longer be guaranteed. In particular, some free messengers pointed out that they do not pass on data and therefore neither consent nor revocation is required.

Another question concerned the possible consequences in the form of **restrictions and disadvantages** for users of the messenger or video service if consent to data processing is not given or revoked. The Bundeskartellamt explicitly asked to what extent functions of the messenger and video service are restricted or other disadvantages arise if consent is not given for one of the seven data categories defined above.

In the case of lack of consent to process **personal data, device/configuration data and location/movement data,** smaller services have stated that their messenger and video service cannot be used without these data. Other services explain that in this case certain functions would be restricted, such as sharing location with other users or using geofilters. Regarding the lack of consent for the processing of **third party contacts or data,** individual major services pointed out that users would not be able to find their "friends" if the contact directory was not synchronised. Other services explained to only provide contact suggestions in a limited automated way. A few smaller messenger and video services stated that users cannot use the service without information about **group memberships, usage behaviour and content.** Other services mentioned relevant recommendations, tags/mentions, alerts, personalised advertising, communication with other users and offline data storage as partial restrictions due to lack of consent or revocation of the processing of this data.
Four services, on the other hand, explicitly stated that there would be no restrictions in Germany even without this data. In addition, some services pointed out that no (video) phone calls or video/voice messages were possible without consent to use the camera or microphone.

d) Informing users about data processing and consent

The vast majority of respondents inform users about the collection, storage and transfer of data as well as consent management in the **privacy policy**. A good quarter of the messenger and video services use their own website for this purpose. Only about one fifth of the services provide the relevant information in the terms of use or the general terms and conditions. The respondents named the relevant links to their information. However, the contents of the information linked in this way could not be checked in detail within the scope of the sector enquiry. As a further source of information on the topic of data processing, some free messenger and video services also mentioned the commissioned data processing contracts or referred to the server operators.

III. Appreciation

The results of the investigation have shown that the technical design of messenger and video services is complex and diverse and is in constant development. An assessment of what is necessary or desirable appears to be a complex undertaking against the background of the manifold preferences of users. In accordance with its mandate in this sector enquiry, the Bundeskartellamt is examining the security criteria primarily from the perspective of the users, which, however, points in the same direction as the interests of the industry on this point (see under 1). The goal of a particularly data protection-friendly service can in principle be achieved in several ways, although there are some criteria that services should always implement. These come from the area of technical data security as well as from data processing (see under 2 and 3). The legal requirements must be complied with (see under 4). In principle, the consumer law sector enquiry is not geared towards individual criticisms of specific industry participants.

Sector enquiries take a look at the **entire industry.** However, on the basis of a checklist for data security and data processing, differences can be identified between the different groups of services that are important for consumers (see under 5).

1. Data protection in the light of consumer and industry interests

The aim of this sector enquiry is to ensure that consumers' data is better protected when they use messenger and video services. Therefore, the situation of users when choosing messenger and video services is first questioned (see section a). The range of services that consumers face should protect their data in the best possible way based on state-of-the-art procedures and be future-proof in terms of data protection, not least if interoperability is to become more important in practice (see section b).

a) Users' perspective

When users are left on their own to choose their messenger and video service, they are faced with numerous criteria according to which they can choose their messenger and video service. The choice can be based on which services are used by friends, acquaintances or recreational institutions such as sports clubs. For many private users, it is particularly relevant that they can take advantage of a free offer and reach as many contacts as possible via the respective service. Other criteria can be certain functions that a service implements particularly well, such as video communication in the group,

or certain settings, such as the language, if communication is to take place with certain nationalities (e.g. relatives from the Asian region as a result of which some foreign services also hold - albeit small - market shares in Germany). Data security and data protection can thus take a back seat as criteria compared to willingness to pay, which they do in many cases (see also Chapter F.II.), even if there are users for whom data protection is particularly important and/or who - in terms of the necessary knowledge - are particularly knowledgeable.

Many of the security criteria outlined in this report cannot be grasped and evaluated by users of a messenger and video service without further expenditure of time, if they are aware of their existence at all. The question of who uses a messenger and video service and for what - i.e. the decision between **"business" and "private**" - is less decisive than it seems at first glance. Therefore, the Bundeskartellamt has included messenger and video services, which are mainly aimed at business customers and charge a fee for their services, in the sector enquiry.

While there is hope among **business customers that** business users will be aware of the applicable data protection laws when making decisions, there is also hope that business users will be aware of the applicable data protection laws when making decisions. Confidentiality and the security of business data are likely to be a stated goal when using messenger and video services for business purposes. It can also be assumed that many business users employ expert staff who accompany and implement the selection and integration of a messenger and video service in accordance with internal guidelines and with a view to data protection laws.

However, it cannot be assumed without further ado that these assumptions are correct in **individual cases.** Perhaps it is not data protection and data security, but the implementation of individual requirements tailored to the business purpose that are in the foreground when choosing a messenger and video service. Perhaps the security of the data is not decisive, but rather certain functions and features or participation via different devices.

That business users choose a privacy-friendly service is also particularly important because **private users may depend on it.** Business customers play a major role as **multipliers. The** customers of a company or learners at schools, universities or other educational institutions are forced to use as participants the messenger and video service through which the company or educational institution organises video conferences or webinars. They usually do not decide on this themselves. As the findings of the investigation have shown, most video conferencing providers allow the respective administrators to make far-reaching decisions about

the settings. Therefore, the respective organisers must be well informed and sensitised and ensure the security and protection of the data of all participants. After all, a service - even if it is actually used for business reasons - can also be used privately, not only by the business user himself or herself, but also by his or her relatives and friends, for example.

If a higher level of data protection is to be achieved across the industry, it is precisely the consumers for whom data protection aspects are less of a priority who must be reached and informed about security criteria. The same applies to the users who make decisions as hosts or administrators for the participants.

b) State of the art and interoperability

A higher level of data protection is not only due to the wishes of the customers. It is also due to the efforts of the offering services to behave in a legally compliant manner and, if necessary, to do more than implement minimum standards. Regardless of whether the demanders can exert the necessary pressure on the supply side, the services should implement data security in the best possible technical way and be prepared for future developments.

German law distinguishes in various laws between the indeterminate legal concepts of the "state of the art in science and technology" (§ 7 para. 2 no. 3 of the Atomic Energy Act), the "state of the art in technology" (§ 5 para. 1 no. 2 of the Federal Immission Control Act) and the "recognised rules of technology" (§ 3 para. 1 of the Technical Work Equipment Act) as safety-related requirements which the respective installations or objects should meet in order to be officially approved.[155] The Federal Constitutional Court interpreted these indeterminate legal terms in the **Kalkar decision**[156] (so-called three-step theory). The legislature is given a certain leeway in the use of these terms. Following the Kalkar decision, a distinction is made between the "state of the art", the "state of the art in science and research" and the "generally recognised rules of the art".

[155] Cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Stand_der_Wissenschaft #Risk assessment.

[156] See BVerfG, decision of 8 August 1978 - 2 BvL 8/77 Rdnr. 90 ff., 96 ff.

Technology"[157] . The strictest standards are set by the state of "science and technology".
The requirements profile is based on the latest technical and scientific findings.
In contrast, the "recognised rules of technology" are associated with the fact that generally scientifically recognised and practically proven knowledge is implemented. The "**state of the art**" is to be placed in the middle. A general recognition already achieved, which is required for the recognised rules of technology, is dispensed with here. However, it is an advanced state of development which may be regarded as assured for the achievement of certain practical protective purposes. The state of the art reflects what is technically necessary, suitable, appropriate and avoidable. The state of the art is - as already mentioned at the beginning - legally defined by way of example in
§ 3 para. 6 Federal Immission Control Act.[158] It is also found in other national laws, such as § 9 para. 1 Telecommunications Act (TKG)[159] , § 13 para. 7 Telemedia Act (TMG)[160] and § 8a para. 1 sentence 2 BSI Act (BSI-G)[161] as well as for the classification of encryption measures in the annex to § 9 BDSG[162] old version.
The state of the art has also found its way into **data protection legislation.** For the suitability of technical and organisational measures pursuant to Art. 32 (1) of the GDPR, a weighing up is required alongside

---

[157] Examples of recognised rules of technology are the DIN regulations of the Building Standards Committee of the German Institute for Standardisation (Deutsches Institut für Normung e.V.), the regulations of the Association of German Electrical Engineers (Verband Deutscher Elektrotechniker e.V. - VDE regulations) and the regulations of the German Technical and Scientific Association for Gas and Water (Deutscher Verein des Gas- und Wasserfaches e.V. - DVGW), but also VDI guidelines and the implementing regulations of the state building codes. The standards, worksheets and guidelines would not always correspond to the current state of technical knowledge. They would not always contain rules that have been tried and tested over the long term. Therefore, higher-quality services may also be required, cf. *KomNet*, available at: https://www.komnet.nrw.de/_sitetools/dialog/43529.

[158] See *Federal Ministry of Justice*, available at https://www.gesetze-im-internet.de/bimschg/. Cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Stand_der_Technik#cite_note-5, *Der Bausachverständige*, available at: https://www.derbausv.de/zeitschrift/aktuelle-ausgabe/was-sind-allgemein-anerkannte-regeln-der-technik/ and Heise, available at: https://www.heise.de/select/ix/2017/7/1499358051209829.

[159] Telecommunications Act, available at: https://dejure.org/gesetze/TKG.

[160] Telemedia Act, available at: https://de.wikipedia.org/wiki/Telemediengesetz.

[161] BSI Act, available at: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.

[162] Federal Data Protection Act, expired on 25 May 2018 due to the Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and the Implementation of Directive (EU) 2016/680 (Data Protection Adaptation and Implementation Act EU - DSAnpUG-EU).

further criteria[163] according to the "state of the art". Even though a definition of the state of the art is missing in the GDPR, the reference to the term is interpreted as a dynamisation of the GDPR.[164]
Both for a digital industry with a high speed of development and the authorities involved, it is relevant how the "state of the art" is to be interpreted at a certain point in time. The BSI explains that this can be determined on the basis of existing national or international standards and norms from, for example, DIN, ISO, DKE or ISO/IEC, or on the basis of models for the respective area that have been successfully tested in practice. The state of the art is not only a common legal term, but also a proven assessment standard for technical issues. **Technical development is faster than legislation**. Therefore, in many areas of law, it has proven successful for many years to refer to the "state of the art" in laws instead of trying to lay down concrete technical requirements in the law. Since the necessary technical measures can differ depending on the specific case, it is not possible to describe the "state of the art" in a generally valid and conclusive manner.[165]
In classifying the results of the investigation, the Bundeskartellamt follows the prevailing opinion in data protection jurisprudence and the view of the BSI. In particular, this is also done against the background of the **interoperability regulation,** which has found its way into the **Digital Markets Act, which** came into force on 1 November 2022. Messenger and video services will be affected to varying degrees by the new regulations. This will certainly depend primarily on whether a messenger and video service is designated as a central platform service of a company classified as a gatekeeper, which serves as an important gateway for commercial users. This must be an interoperable standard offer - in the wording of Art. 7 para. 4 DMA
"reference offer" - provide. But regardless of whether a service will act as a gatekeeper or request access to the same, the current technical design will influence whether much or little effort is required to ensure the security and protection of data.

---

[163] implementation costs, the nature, scope, circumstances and purposes of the processing and the likelihood and severity of the risk to the rights and freedoms of natural persons, cf. *Simitis, Spiros, Hornung, Gerrit, Döhmann, Indra,* Kommentar zum Datenschutzrecht, Artikel 32, 26 , Baden Baden 2019.

[164] Cf. *Simitis, Spiros, Hornung, Gerrit, Döhmann, Indra,* Kommentar zum Datenschutzrecht, Artikel 32, 22 , Baden Baden 2019.

[165] Cf. *BSI*, available at: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Critical-Infrastructures/General-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html.

ensure if participation in an interoperability regime is intended or required. The requirements of data protection laws must be met at all times. Any specifications within the framework of such an **interoperability regime** should refer to the state of the art. The Bundeskartellamt agrees here with the statements of various industry participants who had pointed out these connections in their responses to the Bundeskartellamt's questionnaire (see F.III.5).

Consumers also face new questions about the security and protection of their data in the wake of the interoperability obligation for gatekeepers contained in the Digital Markets Act. This is not only the case if their messenger and video service is designated as a gatekeeper and has to grant access to other messenger services. If their own messenger service requests access, it must also be clarified whether and how the users' data is protected. This means that it must be comprehensible which security criteria have already been implemented and whether and how they can be effective under interoperability.

2. Safety criteria in check - only strong together

Some of the security criteria on which the Bundeskartellamt has determined are - each considered alone - not an indicator of the data protection quality of a service. Rather, the overall picture - or rather the interaction with other criteria - is decisive.

a) Network structure, standards, protocols - a second look is worthwhile

The network structure, cooperation with standardisation organisations and the protocol used, including its visibility as security criteria, cannot be readily assessed by most consumers and related to data protection quality. First of all, this requires the necessary awareness of the problem and an understanding and interest beyond general knowledge, as well as considerable expenditure of time, to even find out whether the information is available or not, i.e. whether the messenger and video services provide the information.

A slight majority of the messenger and video services surveyed by the Bundeskartellamt are based on a centralised network structure. Users must then log on to the service provider's server and also use its client (app, software). All major decisions are thus in the hands of the service provider.

The type of **network structure** alone does not indicate a clear statement on the data protection quality of a service. It can be an indicator of independence from the service provider itself, especially with regard to the whereabouts of meta-data. The network structure also plays a role with regard to possible interoperability, namely in the question of how a

cross-server communication can be implemented. According to the BSI, the development of corresponding concepts for federated systems is still in its infancy.[166]

A federated network structure is primarily associated with **free messenger systems.** In federated systems, meta-data is not centrally generated, but is generally stored by the respective server operators of the users. However, consumers should be aware that every free messaging system can also be operated centrally as an isolated solution, e.g. within a company or an association. It is therefore important to look closely at who bears responsibility for data security and data protection and how this is perceived when the free protocols XMPP or Matrix are advertised. The free messaging system Matrix in particular can be used as an example to promote a differentiated view. According to the basic concept of Matrix, chat rooms are replicated on all servers involved in the respective chat.[167] This means that the respective data is available on all servers, not only on the users' home server.

If messenger and video services use standards, e.g. from the IETF, this can be a quality signal for users. Cooperation with **standardisation organisations** is widespread in the industry. However, this cooperation can take different forms.

Some of the leading services that are linked to large corporations are involved at the international level and set their own impulses in terms of technical development. Almost all messenger and video services use standardised techniques, even if they have not developed and significantly influenced them themselves. The **double ratchet protocol**[168] for exchange and the **WebRTC standard** for audio/video communication are particularly worth mentioning here.

The results of the investigation showed that 40 per cent of the messenger and video services surveyed disclose the source code of the **communication protocol** they use. Conversely

---

[166] Cf. *BSI*, available at: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Critical-Infrastructures/General-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html.

[167] See, among others, *Free Messenger*, available at: https://www.freie-messenger.de/sys_matrix/.

[168] It is considered state of the art, as the BSI has also explained in more detail. In addition to the classic security properties of cryptography (confidentiality, integrity, authenticity, availability, (non-) deniability), the protocol has several other security properties that are particularly important for messenger and video services. See *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

More than half of the messenger and video services do not publish the source code of their protocol. The protocol is an essential and central part of a messaging system, its language, so to speak, and thus decisive for how further functions, such as encryption, are implemented. This also concerns data protection aspects. Here, for example, the cryptographic principles and properties should also be considered. Among the services with an observable protocol are many free messenger clients that embody the open source philosophy anyway.

Some other messenger and video services use proprietary and visible protocols in parallel. If the protocol is not visible, this makes it difficult for **third parties to verify**. The comprehensibility of technical information is naturally limited for laypersons, even if it is available. However, in addition to expert users who are committed to data protection and data security and who design websites[169] to inform consumers, there are also expert authorities and institutions that have the necessary technical competence. It is understandable that services that offer messaging and videoconferencing as core services and are paid for it should first protect their developments until they have established themselves on the market and only then submit them to the standardisation organisations. However, the latter should then also happen.

From a security point of view, however, it becomes difficult to understand when - as in the industry of messenger and video services - quite a few industry participants apply standards, but some of them - for example, the protocol - have been **further developed and adapted individually** and these further developments were no longer presented to the standardisation organisations after market penetration. In the investigations, reference was made to the WhatsApp protocol, which was developed on the basis of XMPP. The various further developments had been made with the "developer's".

public" was no longer shared. Rather, a closed system had been designed. Such developments are also disadvantageous for any **interoperability efforts**, e.g. in questions of end-to-end encryption across messenger borders.

Safety audits by well-known or less well-known institutions can only offer a **limited substitute for a lack of visibility** here, as the variety of options makes comparisons difficult and very comprehensive knowledge of the various audit procedures is necessary on the part of the auditing third parties in order to be able to derive assessments.

[169] Cf. e.g. E.g. *Free Messenger*, available at: https://www.freie-messenger.de/, *Kuketz*, available at: https://www.kuketz-blog.de/, *Golem*, available at https://www.golem.de/sonstiges/leitbild.html and much more.

b) Encryption - everything goes, nothing must?

As shown in section D.I.4.a), messenger and video services can protect users' data during transmission in two different ways. Transport encryption makes it impossible for third parties to read the data sent during transmission between the user's client and the server. However, the server operator still has access to the data because it is available on the server in plain text. To prevent this, according to the BSI, "additional encryption of the content between the end points of communication, i.e. the user clients of the sender and recipient(s) on the end devices, is necessary, which can be achieved by means of end-to-end encryption.
can"[170] .
The Bundeskartellamt has devoted a great deal of space to end-to-end encryption in its investigations, as it is often interpreted by the public as the decisive criterion for data security. Even though it is not the encryption alone that matters, but the interaction with other security criteria, encryption has gained a prominent position due to the temporary media presence in the wake of inaccurate statements about it by individual services. Furthermore, it is often cited as an example of a significant challenge in the context of discussions on interoperability. The Bundeskartellamt has therefore taken a closer look at this security-relevant topic from various aspects.

aa) Group chat and video conferencing

The results of the survey suggest that **text messages** are encrypted throughout the industry, as none of the services surveyed stated that they do not encrypt or cannot encrypt. As shown, the state of the art is now end-to-end encryption, which is ideally combined with transport encryption, which has been standardised for some time.
Some of the known services surveyed have only implemented **transport encryption.** Since many of these services are very popular with consumers, additional end-to-end encryption that corresponds to the state of the art would be desirable here. In its publication "Modern messengers - encrypted today, interoperable tomorrow?

[170] *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

described high effort that encryption currently causes in group chats.[171] Most services that use end-to-end encryption are therefore unable to ensure this when communicating in groups, as the Bundeskartellamt's investigations have confirmed.

As already described above, various protocols or even individual variants of the double ratchet protocol are used in the industry. These individualisations also include encryption as an essential property of the protocol, especially in the case of interoperability, i.e. across messenger borders. Encryption is considered the obstacle most often cited in connection with interoperability. The **MLS standard** is described as the standard that could remove this hurdle, provided the other prerequisites - as mentioned above, suitable interfaces and an adapted network infrastructure - were created. The implementation of the MLS standard by the services remains to be seen. A rapid diffusion in the market would be desirable.

Not only for group chat, but also for **video conferences and webinars,** end-to-end encryption is currently subject to **technical limitations**. In general, end-to-end encryption requires that participants are technically capable of providing and applying the necessary encryption functions. All participants must be on the same security level. Conversely, E2E encryption cannot be achieved if one participant falls below the required security level. This is the case, for example, when participants use a **WebRTC client.** WebRTC is a protocol directly anchored in the browser, which can only encrypt end-to-end between two endpoints. If there are more than two participants in a videoconference, these are the end device of the user with the server of the service, which no longer meets the requirements of end-to-end encryption. These aspects are reflected in the investigation results. According to the industry participants surveyed, the WebRTC protocol is most frequently used to encrypt audio and video telephony. The

[171] Group chats are currently encrypted by encrypting them as individual chats between all group members. For a group with n members, there are n(n-1)/2 of these individual chats, so that the encryption effort grows quadratically with the number of participants and quickly becomes a problem for larger groups (>100 participants), cf. *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

using services have also for the most part indicated that they cannot encrypt video conferences in the group end-to-end.

End-to-end encryption cannot currently be technically linked to certain **features** that users like to use in videoconferences: When users use recording features, dial into a meeting from the public telephone network or a standardised SIP video device, or use an assistant, it is not possible for the services to provide end-to-end encryption. Consumers may interpret these **features as an "indication**"[172] that end-to-end encryption should be questioned if it is advertised or remember the technical limitations when using it.

Large video conferences for **webinars with several hundred participants** cannot currently be technically secured by E2E encryption. In this use case, it is necessary to check whether the service offering the service operates a video service location in Germany and whether this has been security-checked (for example, by a BSI C5 certificate).
Transport encryption and the secure operation of the video service in Germany should be the criteria for this. Furthermore, it must be ensured that the identity of the participants can be established beyond doubt ("authentication"). End-to-end encryption ensures the integrity of the transmitted data. Without prior doubtless authentication, it ensures the protection of the transmitted data, but does not ensure who can receive this data.

bb) Automatic activation

Experts in particular like to point out that not every communication necessarily has to be encrypted (e.g. grandma's cooking recipe) or that this is not desired (e.g. for business reasons). It is also argued that email is mostly used unencrypted. Certainly, IT-savvy consumers or many business users can decide for themselves when they want to encrypt and when they don't and appreciate this freedom. Most consumers, however, are probably not at all aware of the fact that there can be **decision-making options** here. The time required for the corresponding research, combined with a lower appreciation of encryption compared to other features of the desired messenger and video service, is also a factor.

[172] Source: Investigations. Cf. *datenschutz notizen*, available at: https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597/.

service can lead to the fact that encryption is not used. For this reason, **automatically activated end-to-end encryption** should be integrated into the free services for consumers, as far as this is technically possible at present, in order to further improve data security. The option of turning off end-to-end encryption, e.g. for experienced users, could be provided.

The security of end-to-end encryption also depends in particular on **key management.** Ideally, the communicating parties alone should have the keys, not the respective server operator. This is because if the key is generated on the server of the service and then distributed to the end devices, the service operator could decrypt the sent data with the help of the key known to him. Services that have indicated that the key is generated **locally and the private key** remains **on the end device** include many free messenger clients, open source services and also video services.

With the focus on business customers, especially in the case of video services, many user choices go hand in hand with the role of the host. Depending on the model chosen, certain types of encryption and key management can be implemented, among other things. A leading video service points out that key management requires the **establishment of a comprehensive process for the generation, secure storage and secure distribution of keys.**

Loss or compromise of the master key is to be equated with loss or compromise of the complete data stock in the system. Users who are not experts are therefore advised to place this task in the responsibility of the selected service, especially if they, as administrators, define the security framework of an exchange via video for the participants.

c) Other safety aspects

Other security procedures such as encryption of data on the end device, filing encryption, two-factor authentication or the creation of security copies are practised in the industry to some extent. Two-factor authentication as an option and storage encryption are each offered by half of the services. Backups can be created at two-thirds of the services surveyed. Encryption of data on the end device is practised by slightly less than two-thirds of the respondents. **Efforts to achieve a higher degree of diffusion** appear necessary for all of these security procedures.

Via **two-factor authentication,** users can authenticate themselves to their messenger and video services if the respective messenger system is open for this procedure. Their identity is proven via two different components that

from the categories of knowledge (e.g. password, PIN, answer to security question), possession (e.g. smartcard, TAN list) or biometrics (e.g. fingerprint, facial recognition). Similar to end-to-end encryption, users must actively choose this option if they want to use it. Here, it would be advantageous for data security if two-factor authentication, especially for versions of applications that consumers prefer (e.g. free offers, trial offers providing basic functions) would be preset. The systems that have not integrated the procedure so far should make an effort to open it up accordingly.

With the other security aspects mentioned above, a higher degree of diffusion in the industry would also be desirable. Encryption, for example, is only complete when **encryption of the data on the end device and also, in particular, storage encryption is** set up, i.e. when the data stored in the end device is also encrypted. The services that are active here use state-of-the-art AES[173] and RSA[174] procedures. In addition, the various messenger and video services sometimes have **individual regulations and requirements that** must be observed, which can make the application challenging for users. It is not uncommon for encryption to be tied to the type of end device or operating system or the selected function or type of encryption. Consumers need to look carefully to see whether or not encryption is provided on the terminal device when they choose to use the app. Some services refer to the possibilities of the operating systems that consumers can use for filing encryption

[173] See also chapter D.I.4.a, Advanced Encryption Standard (AES). The standard is usually implemented together with other encryption methods, e.g. also as the basis of transport encryption. The AES encryption method is a block cipher whose block size depends on the AES encryption variant. The variants of the AES encryption, AES-128, AES-192 and AES-256 contain the length of the key in bits in their designation. The most secure AES variant is therefore AES-256.

[174] See also chapter D.I.4.a. The RSA method (named after the developers R. Rivest, A. Shamir and L. Adleman) is a well-known asymmetric encryption method. With the RSA method, digital data can be converted and made unrecognisable using a specific algorithm. The so-called RSA key is necessary for decryption. However, not the same key is used for encryption and decryption, but a key pair. This consists of a private key and the public key. The private key must be kept secret for secure RSA encryption.

The situation is comparable for **backup copies.** Many services offer this function, but with varying scope and requirements. With some services, consumers have to invest a lot of time and effort because various details and requirements have to be observed.
In any case, it would be beneficial for data security if the aforementioned security procedures were integrated by those services that have not done so so far. In any case, it should be clearly communicated which options users can take themselves to protect and secure their data on the end device.

3. The crux with the (meta-) data

The Federal Cartel Office asked the messenger and video services questions not only about technical security but also about data processing. This was intended to provide an overview of industry-wide practices. The practices of individual messenger and video services have been the subject of intense public discussion and criticism for a long time and have also been the subject of official proceedings in some cases. Whether and to what extent there could be a need for further investigation of legal issues throughout the industry should be able to be assessed through the investigations within the framework of the sector enquiry.
For the purposes of the sector enquiry on "Data Processing", the Bundeskartellamt has defined the data categories "Personal Data", "Device and Configuration Data", "Location and Movement Data", "Third Party Contacts/Data", "Group Memberships", "Usage Behaviour" and "contents" were formed (see Figure 9 in Chapter D.II.4). These categories should include unencrypted, encrypted but also (partially) anonymised, hashed, supplemented, enriched or generated data.
The so-called meta-data were not explicitly marked. **Meta-data** is structured data that contains information about characteristics of other data.[175] For example, they include information about when someone is online and how many devices they use, which contacts exist and which IP addresses they have.[176] Meta data is always generated when communicating via messenger and video services. This can have a technical cause, for example, and concerns e. g.
B. the server, the time and duration of the connections with the clients of the users.

---

[175] Cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Metadaten.

[176] Cf. e.g. E.g. *Initiative freie Messenger*, available at https://www.freie-messenger.de/geheim nisse/privat/.

user is registered.[177] There is scope for other (meta) data. Their collection only serves internal purposes of the messenger and video services and could be avoided.

Meta data can be used by messenger and video services for various **purposes**,

z. For example, to improve the functioning of the service. But they can also be used to create user profiles or to place personalised advertising. As mentioned at the beginning of this chapter, some popular services are seen by the public as the epitome of a business model in which data is collected for own advertising purposes, especially **personalised advertising and the creation of user profiles, or for passing on to third parties.**

The result of the Bundeskartellamt's investigations was that almost all of the messenger and video services collect data for the functionality of the service, according to their own statements. This mainly concerns personal data and device/configuration data. More than half of the services also collect data on "usage behaviour", "group memberships", "third-party contacts/data" and "content".

Still, about one third of the services collect "location/movement data" of the users for the functionality of the service. The handling of consumer contacts and third party data by the services becomes virulent when uploading the contact directory and is the subject of a legal examination in the following chapter D.III.4.

In the case of another much-discussed topic - the **passing on of data to third parties - the** aim was also to gain an industry-wide overview, since detailed analyses can only be, and have already been, the subject of individual proceedings, possibly also on the basis of other legal bases. For the purposes of the sector enquiry, the question was asked in particular about the **transfer of data to the large internet groups**. Only one service indicated in the survey that it passed on personal data (zoom) or device/configuration data to Facebook (now operating under the name "Meta"), in some cases with reference to the explicit consent of the users. The forwarding of data to Google was confirmed somewhat more frequently. The same applies to data analysts. Otherwise, according to the information provided, individual services transfer data to subcontractors, law enforcement agencies or "business partners". According to this, personal data, device information and data on the

User behaviour data. Since among the industry participants - as already mentioned several times - there are some large corporations that are active in markets that also affect messaging and videoconferencing (e. g.

[177] If meta-data is to remain confidential and not be stored on servers, the participants would have to connect directly with each other and not use a server. (An example of this is the Briar system. Cf. *Briar*, available at: https://briarproject.org/).

operating systems, communication technology) have a strong position, **internal data sharing** deserves special attention.

Information about purposes of data collection and data sharing is not available to consumers in an easily accessible way.[178] In principle, the **privacy policy** should describe the extent to which meta-data is collected and when it is deleted. However, studying them requires some time and the willingness to struggle through texts that tend to be difficult to read. According to the Bundeskartellamt's experience in other sector enquiries, consumers usually do not invest enough time to comprehend all the contents and providers often do not take the necessary care in formulating the relevant texts.[179] **The data thriftiness of a service** could be derived from further indications, the development of which, however, also requires some effort from the users. The **business model** could be considered as a kind of first **indication of the purpose of the data collection** and the extent of the data transfer. After that, the use of the data for advertising purposes would give rise to concerns. However, consumers are also not sufficiently aware of the business model for the majority of messenger and video services. In addition, an **accessible source code**[180] could also provide information about the data minimisation of a service. However, the analysis here - as already explained - naturally requires not only access to information, but in particular professional knowledge and expertise and again a lot of time to be able to make assessments.[181]

At least in comparison, information **about the location of the server** could be better understood here, which also allows conclusions to be drawn about the data thriftiness of a messenger and video service. Data protection laws vary around the world. If the server(s) of a messenger and video service are located in Germany or the EU, the European Data Protection Regulation applies, with which, in comparison to

---

[178] See on the high demands on consumers in the search for information under F.II. and G.II.2.

[179] Cf. *Bundeskartellamt*, Sector Inquiry Smart TV, July 2020, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf? blob=publicationFile&v=5. See also F.II.

[180] In chapter D.I.1.b it was shown that the source code of the server and client can be viewed by slightly more than 40 per cent of the services surveyed, especially in the case of free messenger clients, open source services and services that explicitly advertise data protection.

[181] Cf. *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/ messenger.html.

other jurisdictions are accompanied by high data protection requirements. However, it cannot be assumed that all consumers are aware of this connection and that there is interest in it. Furthermore, it is also true here that the information must be sought out, as it is generally not centrally placed on the websites of messenger and video services.

The Bundeskartellamt's investigations suggest that a clear majority of the messenger and video services surveyed store their data outside the EU. Seven services explicitly stated that they store at least one category of data only in the USA. Some services maintain storage infrastructures in the EU and in third countries, especially the USA. It remained partly unclear where EU citizens' data is transferred to.

Due to the **different data protection standards in the European Union and the USA**, which are closely linked economically, especially in the digital economy, the legal assessment of this question is of particular importance. This is also made clear by ongoing discussions and activities in the (specialist) public. The Bundeskartellamt is therefore taking up this aspect in a separate legal analysis (see the following section D.III.4).

An essential aspect of secure messenger and video services against this background is also the **deletion of** data, which is not handled uniformly in the industry, as the investigation results show. There are not only major differences between messenger and video services. Also internally, practices in messenger and video services can differ by type of data category, by business or private use, or by type of function (video recordings, voice messages or other content).

Whenever **user accounts** have to be created in order to use a service, consumers are required to enter extensive data. In contrast, there are services that do not require the creation of accounts. Those who choose to use them can thus limit the disclosure of personal data. When it comes to **deleting an account**, server administrators or users decide on the process. When open source services are used, the question often does not arise because accounts do not have to be created in the first place. Some services delete data automatically after the end of the contract or account closure, others also at the request of the user.

Finally, the **integration into the operating system** also influences what happens to the meta data. Even if meta data is deleted promptly by the service, it can still be stored by the operating system of the end device, typically iOS/iPadOS (Apple) or Android (Google) in the case of mobile devices and smartphones in particular. This is the case, for example, when push messages indicating the receipt of a new message are sent.

When the Digital Markets Act comes into force on 1 November 2022, data processing could become even more of a focus due to the interoperability obligation of gatekeepers. If cross-messenger exchange is practised and the users' data is passed through several hands, the requirements for data security will increase. Responsibilities will have to be clarified (see Chapter F.IV.4) For consumers, the (data protection) assessment of messenger and video services is likely to become even more challenging than it already is.

4. Legal classification

As already indicated in the discussion of the individual security criteria and data processing, the aforementioned data handling practices may not only lead to security deficits in a very practical way. They can also violate applicable consumer law. The analysis of selected legal issues is the subject of this chapter.

The legal framework is provided by the Unfair Competition Act and the General Data Protection Regulation. In addition, the scope of the sector enquiry instrument is briefly referred to (again) in this legal context. Subsequently, the focus is on the concrete legal issues. In doing so, the Bundeskartellamt focuses on aspects that are particularly important for consumers in messaging and videoconferencing and to which they should and can pay special attention. After a brief introduction to the legal framework (see a)), three legal issues are addressed. On the one hand, this concerns the handling of consumers' contacts when the contact directory is uploaded and synchronised (on this under b)). Secondly, it will be discussed how an international data transfer including data storage of the services must look like if the current case law based on the GDPR is taken into account (see c)).

Finally, it is a question of violations of the law of fair trading and the question of whether the services have the

transparency requirement or mislead consumers by withholding information (see d)).

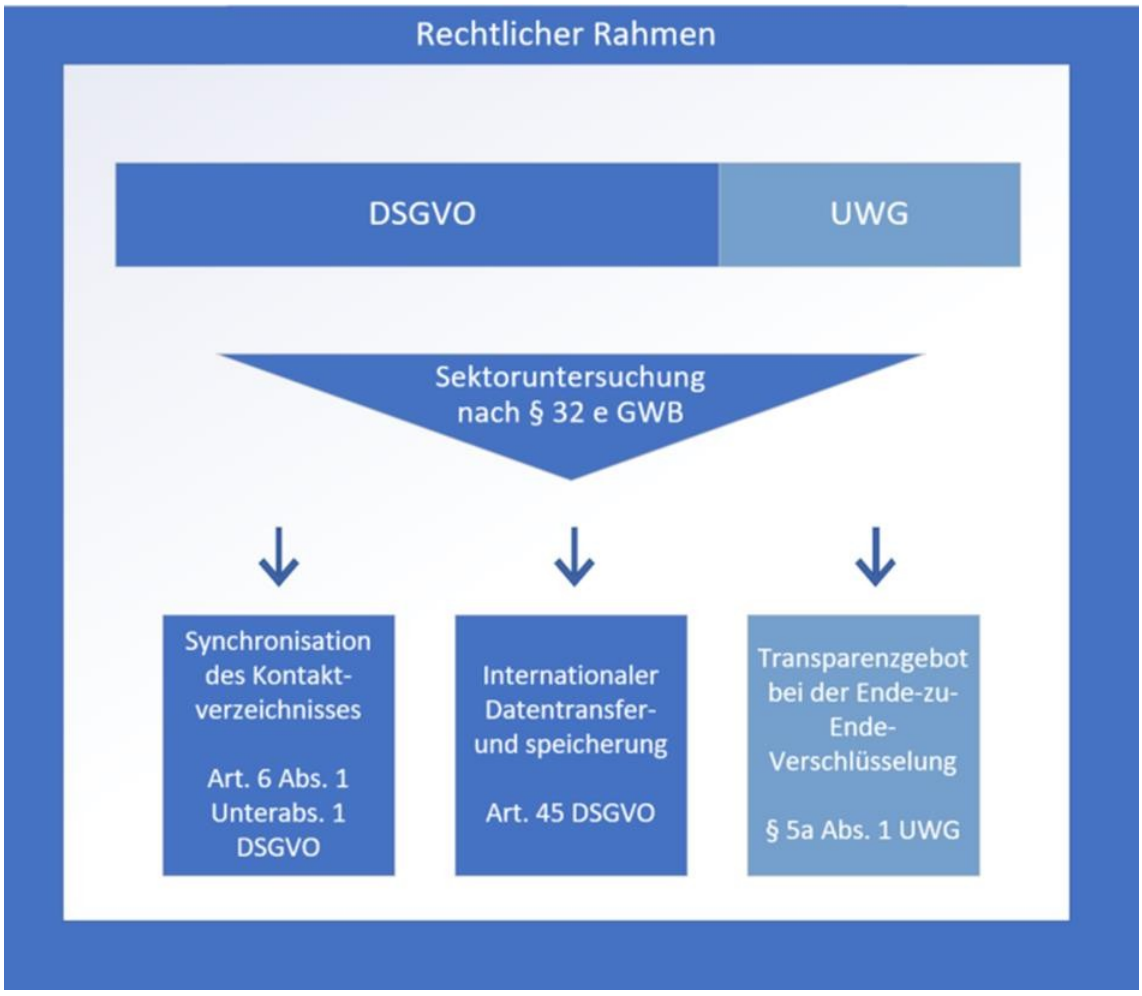


Figure 12: Legal framework and legal topics of investigation

a) Legal framework

The practices of messenger and video services must be measured against the provisions of the **UWG.** According to Section 1 (1) UWG, its aim is to protect not only competitors and other market participants, but also consumers from unfair business practices. According to Section 1 (2) UWG, the interest of the general public in undistorted competition is also worthy of protection. In the legislative materials on the new powers of the Bundeskartellamt under Section 32e (5) GWB, the UWG is explicitly mentioned.

The relevant legal bases are essentially Section 5 (1) UWG (misleading commercial acts) and Section 5a (1) UWG (misleading by omission).

As a further legal basis, the **GDPR has** applied in Germany and the entire European Union since 25 May 2018. The GDPR is currently the legal framework for the classification of

data protection violations and also forms the essential standard of review in data protection issues in the following explanations. Decisive for the
The applicability of the GDPR is the "processing" of so-called "personal data" (Art. 4 No. 1 GDPR). However, in the sector enquiry into messenger and video services, the Bundeskartellamt cannot subsume individual cases under the aforementioned provisions and thereby include all messenger and video services under consideration. This is because the depth of examination of a sector enquiry under consumer law as an advisory and analysing instrument is limited compared to administrative proceedings within the meaning of Section 54 (1), (2) no. 2 ARC, which are directed *against* a company. Thus, for the **court-proof proof of a violation of consumer law** by a certain messenger and video service, it would be necessary in particular to clarify the concrete circumstances in the individual case and, if applicable, also the respective expectations of the consumers.
Providing such evidence against a company in an individual case would exceed the possibilities of the present sector enquiry. An **administrative procedure** directed against an individual company would be the right instrument for prosecuting the violations. There, the affected messenger and video services would also have corresponding rights of defence. In addition, business and trade secrets could be cited to a greater extent in the decision on such proceedings than is possible in a sector inquiry report intended for the general public. The same applies, if applicable, to undertakings of the companies that can be accepted for resolution in an administrative proceeding.
However, the Bundeskartellamt was initially deliberately not given such enforcement powers in consumer protection within the framework of the 9th GWB amendment.

b) Synchronisation of the contact directory

According to the results of the investigations, almost one third of the messenger and video services surveyed generally synchronise the contact directory of users, including widely used services such as Facebook Messenger, Skype, Snapchat, Threema, WhatsApp and Zoom (see D.II.2.b) for the results of the investigations). The **telephone numbers of the users' contact persons** are recorded, but not necessarily their other contact information. The users must first agree to this process, which is later repeated automatically at intervals.
Such contact persons of the users who do not use the service ("non-user"), but whose telephone numbers are included in the synchronised contact directory, necessarily do not consent to their collection vis-à-vis the messenger and video service concerned, as it is unknown to them to date. The consent of non-users

cannot be constructed by the fact that it is implied when a telephone number is passed on. Non-users cannot be presumed to anticipate that the phone number will reach one or more messenger and video services through a synchronisation process via the entry in a contact directory of a mobile phone.[182] However, the service is also responsible for compliance with the GDPR with regard to the synchronisation of the telephone number of non-users and therefore requires a different legitimisation for this processing operation. The service cannot rely on the fact that the user is responsible for obtaining consent from the non-users among his or her own contacts and that the service is only a processor in this respect.

The fact that the messenger and video service in question is likely to play the role of a **controller within the meaning of Article 4(7) of the GDPR in** this context and not merely a processor (for the user) under **Article 4(**8) follows from the following:

The controller is the body which alone or jointly with others determines the purposes and means of the processing of personal data. According to the provisions of the

Art. 29 - Data Protection Working Party, the demarcation from the processor is about the allocation of responsibility in a typified form. Therefore, the focus must be on why the data processing process takes place and who initiated it.

Responsibility is to be allocated where the factual influence lies; only technical issues

can be delegated to the processor, not essential questions such as "what data should be collected".[183]

The inclusion of phone numbers of non-users in the contact directory by the messenger and video service serves to automatically display users who join later among their contacts immediately after their registration. Although this may result in added value for users, the **actual influence** over the entire process lies with the messenger and video service, which created this feature during the development of its product and controls the technical processes. The user, on the other hand, cannot even find out with a reasonable amount of effort which of his or her own

[182] Rejecting also AG Bad Hersfeld, decision of 20.03.2017, Az. F111/17 EASO, para. 96, 107.

[183] Cf. Art. 29 Data Protection Working Party, Opinion 1/2020, p. 40 ff.

contacts already use the service or not. The **responsibility under data protection law** therefore lies with the service concerned.[184]

In this context, legally compliant action by the service requires legitimation under data protection law in accordance with Art. 6 (1) subpara. 1 DSGVO.

The phone number of the non-user is without further ado a personal data in the sense of Art. 4 No. 1 DSGVO. Uploading and storing it is processing according to Art. 4 No. 2 DSGVO. Even if a service does not collect any further information about the non-user besides the telephone number, it is nevertheless a personal data because the non-user is already identifiable with it. Thus, the service can research further information about him or her by means of a call or a search in social networks.[185] The reference to a person also does not cease to exist where a service creates a cryptographic hash value after collecting the non-user's telephone number and then irrevocably deletes the telephone number itself. This applies in any case if this hash value is stored with others in a list that is in turn linked to those users from whose contact directories the original phone numbers originate.[186] In this way, messenger and video services can inform the specific user as soon as non-users among their contacts become users, so that there is a personal reference. Legitimisation by consent of the non-user according to Art. 6 (1) subpara. 1 a) DSGVO is not possible. Alternatively, legitimation can be derived from lit. f), according to which - in short - the processing is necessary to protect the legitimate interests of the controller or a third party in **consideration of the data subject's rights to freedom.** However, deriving legitimacy on the basis of legitimate interests is likely to be difficult here or at least require a great deal of effort to justify.

A successful justification may still succeed for the **short-term uploading of telephone numbers** from the contact directory. This is because it is possible to determine which of them belongs to a contact who is already registered with the service, so that the user can subsequently be informed.

---

[184] Cf. in detail Data Protection Commission/Ireland, decision of 20.08.2021, ref. IN-18-12-2, para. 145. "*WhatsApp Ireland Limited*.

[185] Cf. Data Protection Commission/Ireland, decision of 20.08.2021, ref. IN-18-12-2, para. 83, 91 "*WhatsApp Ireland Limited*".

[186] European Data Protection Board, Binding Resolution under Art. 65 GDPR No. 1/2021 of 28.07.2021, para. 156.

to indicate this. If the telephone numbers of non-users collected on this occasion are subsequently deleted, their interests in protection are unlikely to outweigh the service's interest in efficient networking.

This does not necessarily apply to the subsequent storage of the telephone number of non-users, whether in clear or hashed form. The networking advantage generated in this way is only slight. The subsequent information of the user about new users among his or her contacts can in principle also take place without the **long-term storage of telephone numbers in question.** As soon as the previous non-user is registered and has agreed to the processing of the data, he or she can be displayed as a new user during the next readout of the contact directory. Assuming daily synchronisation, the remaining delay compared to the immediate notification after registration of the previous non-user should hardly be significant. If the telephone numbers of the non-users are stored by the service, it runs a high risk that its interest in an efficient networking possibility and the attractiveness of its product will be outweighed by the rights of the non-user.

c) International data transfer / data storage

The Bundeskartellamt did not only focus its investigations on the specific legal issues under investigation. It also sought to get a comprehensive overview of the data processing process of the messenger and video services. Leading services are under constant criticism in this context. Therefore, it seemed appropriate to also query the practices of the other industry participants. In this way, responses from the services on the question of data storage and thus also on data transfer were also collected.

In the Bundeskartellamt's preliminary view according to the results of the investigation, some messenger and video services are at risk here of not behaving in a legally compliant manner. This primarily concerns those services that store the data of German users in the USA. In the following, the applicable legal framework will first be explained (see aa), before - based on the results of the investigation - the special legal requirements for data transfers to the USA will be discussed (see bb).

aa) Legal basis of international data transfer in the European Union

The protection of personal data of European Union (EU) citizens by the rules of the GDPR goes beyond EU borders. The messenger and video services - which

respective data controllers - must check whether the general requirements for a data transfer - also for the purpose of data storage in a third country - are met.

For example, data may only be transferred to countries outside the EU and the European Economic Area if it is ensured that there is an **adequate level of data protection in** the so-called third country (Art. 45 GDPR). According to Chapter V of the GDPR, this level of data protection can be ensured or achieved in various ways. Data can be transferred on the basis of so-called

The European Commission currently has adequacy decisions with Andorra, Argentina, the Faroe Islands, the United Kingdom and Guernsey.[187] The European Commission currently has adequacy decisions with Andorra, Argentina, Faroe Islands, Great Britain, Guernsey, Israel, Isle of Man, Japan, Jersey, Canada, New Zealand, South Korea, Switzerland and Uruguay.[188] The so-called data protection shield (EU-US Privacy Shield), which the EU had agreed with the USA, is no longer in force.

If no adequacy decision exists, this means that the respective third country or organisation does not offer an adequate level of protection. If data is nevertheless to be transferred, this must be accompanied by further protective measures - **guarantees according to Art. 46 GDPR. The** data transfer can be secured with standard data protection clauses or binding internal data protection rules (Binding Corporate Rules, BCR) as well as approved codes of conduct / certification mechanisms.[189]

The **standard data protection clauses** can be issued by the European Commission or other European supervisory authorities. In addition, individual contractual clauses are also possible to secure a data transfer. The European Commission issued standard contractual clauses in June 2021.[190] Since 27 September 2021, only the current clauses are to be used. Standard data protection clauses of other supervisory authorities and individually negotiated

---

[187] Cf. *BfDi* on international data transfer, available at: https://www.bfdi.bund.de/EN/Fachhemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html;jsessionid=4FF79D8D39D5B5ED7D0E9734B6AD8F99.intranet242.

[188] Cf. *European Commission*, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[189] Further mechanisms are provided for public authorities. For example, they can use international agreements or use an administrative arrangement. Both must provide enforceable data protection rights and remedies to data subjects. The European Data Protection Board has developed guidelines on this. Authorities with law enforcement functions transfer data on the basis of the Federal Data Protection Act.

[190] See Implementing Decision EU 2021/914, available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

Clauses must be agreed in the European circle and approved by the EU Commission.[191]

If data is to be transferred to third countries, **binding internal data protection rules (Binding Corporate Rules, BCR)** can also secure the transfer. This instrument is mainly used by internationally active corporations with internal data flows, including to third countries. It is based on rules on how to handle personal data. These rules must be linked to enforceable rights for the data subjects. They must apply to the entire group of companies, i.e. be legally binding. The respective national supervisory authority must coordinate with the European partners and obtain approval from the European Commission.[192]

The situation is similar for industry-wide **codes of conduct** or **certification mechanisms** approved by the competent supervisory authority. Corresponding guidelines are in process at the European Data Protection Board.

If neither an adequacy decision nor appropriate safeguards exist, a data transfer to a third country may exceptionally be permitted as a **strict exception under Art. 49 GDPR.** This is limited to special explicitly mentioned constellations, e.g. if the data transfer is necessary for important reasons of public interest. According to the explanations of the Federal Commissioner for Data Protection, Art. 49 is to be interpreted narrowly and may not be used for regular data transfers that affect a large number of individuals.[193]

bb) Investigation results in the light of current case law on data transfer to the USA

As mentioned in the previous section, the Privacy Shield - the adequacy decision for the US - is no longer legally binding.

The European Court of Justice issued a landmark ruling on international data transfer in the summer of 2020, which initially led to great uncertainty about the extent to which a data-based

---

[191] See *BfDi* on standard data protection clauses, available at: https://www.bfdi.bund.de/DE/Fachthemen/content/europe-international/international_data_transfer.html;jsessionid=4FF79D8D39D5B5ED7D0E9734B6AD8F99.intranet242.

[192] Cf. on the authorisation procedure for binding internal data protection rules *European Commission*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

[193] Cf. *BfDI* on exceptions under Art. 49 DSGVO at: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-International/Internationaler_Datentransfer.html.

cooperation with the USA can still take place. In the so-called **Schrems II ruling**[194] , the European Court of Justice had confirmed that personal data of EU citizens transferred to a third country must receive "essentially equivalent protection" there as under the European GDPR. The ECJ denied an essentially equivalent **level of** data protection for the **US level of protection.**[195] In the course of this, the EU Commission's adequacy decision on the EU-US Privacy Shield (Privacy Shield Decision 2016/1250) was declared invalid. As a result, personal data may no longer be transferred to the USA under the Privacy Shield.

In contrast, the court declared the EU Commission's decision on **standard contractual clauses and BCRs to** be effective as an appropriate guarantee. However, **additional measures** must then be taken to protect the data of EU citizens from unrestricted access by US security authorities. The additional measures can in principle be based on

technical, organisational and / or legal level must be implemented. The court emphasised that these must then also be effective and practically available in the third country.

In addition, data may still be transferred in **exceptional cases under Art. 49 GDPR**, provided that the rule-exception relationship envisaged by the GDPR is respected and the conditions set out in Art. 49 would be met (e.g. requirements for an explicit, informed and voluntary decision).[196]

The court did not grant a transitional period.

The background to the proceedings were the activities of civil rights and data protection activist Max Schrems, who has been taking action against Meta for several years. Using the example of the US platform

---

[194] Case C-311/18 "Schrems II", available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN.

[195] See *Der Bundesbeauftragte für den Datenschutz*, Information letter on the impact of ECJ case law on international data transfers (Case C-311/18 "Schrems"), 08 October 2020, available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2020/Rundschreiben-Information-Schrems-II.html?nn=339632.

[196] See *Der Bundesbeauftragte für den Datenschutz*, Information letter on the impact of ECJ case law on international data transfers (Case C-311/18 "Schrems"), 08 October 2020, available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2020/Rundschreiben-Information-Schrems-II.html?nn=339632.

it has the courts review whether personal data of EU citizens may be transferred to countries outside the EU (and the EEA).[197] In 2015, in the course of such proceedings - the so-called **Schrems I ruling**[198] of the ECJ - the Safe Harbour agreement, the predecessor of the Privacy Shield - was declared invalid. Since the "Schrems II" ruling was issued, a new complaint by Max Schrems against Meta has been heard by the Austrian Supreme Court (OGH), but it has less to do with the question of legally compliant data transfers.

In the wake of the Schrems II ruling, data controllers within the services must review their data transfers to countries outside the European Union and, if necessary, base them on a new basis. If appropriate safeguards according to Art. 46 GDPR are used, it must be checked whether and which additional measures are necessary to protect the data in the third country. The result of the check must be documented. The **documentation** must be designed in such a way that the supervisory authority can understand that the provisions of the GDPR are being complied with. If the result of the audit is that the data transfer is not permitted, but the transfer is continued, this must be reported to the Federal Commissioner for Data Protection.

According to the results of the investigations, a number of services store at least one category of data only in the USA (see D.II.3.).[199]

Since the US Privacy Shield has been declared ineffective by the European Court of Justice, the transfer of data to the US would be impermissible unless it is secured by appropriate safeguards including additional measures. The suspicion of inadmissible practices in international data transfer under the GDPR cannot be dispelled at this point. The Federal Cartel Office

---

[197] Cf. Handelsblatt, available at: https://veranstaltungen.handelsblatt.com/cybersecurity/internationaler-datentransfer-nach-schrems-ii/.

[198] Case C-362/14 "Schrems I", available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-362/14.

[199] Furthermore, insofar as a quarter of the respondents stated that they store at least one category of data in a public cloud of technology companies based outside the EU, this does not necessarily mean that data is stored in the USA. Thus, the Higher Regional Court of Karlsruhe ruled in the context of public procurement law that the mere fact that a subsidiary of a US group is commissioned does not mean that it can be assumed that, due to the group relationship, instructions will be given to the subsidiary that are contrary to the law and the contract or that the European subsidiary will follow instructions of the US parent company that are contrary to the law through its managing directors, see OLG Karlsruhe, decision of 7 August 2022, ref. no. 15 Verg 8/22, openJur 2022, 16869.

there is no information on the extent to which the data transfer to the USA is secured by the messenger and video services concerned with guarantees and additional measures. The European Commission does provide an overview[200] of which companies have approved binding internal data protection regulations (BCR). However, only one of the messenger and video services questioned by the Bundeskartellamt was on this list, but it had - at least not explicitly - stated in the investigation results that it stored data of EU citizens in the USA.

The use of standard contractual clauses and the additional measures required by the ECJ were not addressed by the services in their responses.

cc) New privacy shield on the way?

Since the Schrems II ruling in July 2020, the EU and the US have been negotiating a **new Privacy Shield.** It is intended to allow the transfer of personal data of EU citizens to recipients located in the USA. An "agreement in principle" was reached at the end of March 2022.

A legal text and more detailed information are not yet available. In a joint statement, both sides said that new rules would limit US intelligence agencies' access to data to what is necessary and proportionate to pursue defined national security objectives. In addition, there would be an independent redress mechanism to investigate complaints from EU citizens about data access by US intelligence agencies and to order remedial action.[201]

It therefore remains to be seen when data transfers to the USA will be placed on a new legal basis and what regulations will be agreed in detail.

d) Lack of information in connection with end-to-end encryption

The Bundeskartellamt has devoted a lot of space in its investigations to encryption, especially as an essential technical element for data security and thus also for data protection. In the past, security deficiencies in messenger and video services have repeatedly come to light in the

---

[200] See *European Commission,* available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

[201] See Joint Declaration of the *European Commission* and the *United States* on the Transatlantic Privacy Framework of 25 March 2022, available at: https://ec.europa.eu/commission/presscorner/detail/de/IP_22_2087. See also *MDR*, available at: https://www.mdr.de/nachrichten/welt/politik/datenschutz-abkommen-einigung-europa-usa-privacy-shield-100.html.

The issue was raised in connection with encryption. As already explained in D.I.4.a)cc), an individual interpretation of **end-to-end encryption** had attracted attention at one video conference provider, which did not correspond to the actual technical definition of end-to-end encryption. It is possible that encryption gained its prominent position among security aspects due to this temporary media presence. In any case, it is often perceived by the public as the decisive criterion for data security, while other aspects described in this report are not mentioned publicly. In the context of discussions on interoperability, encryption has also regularly been used as an example to illustrate the particular challenges of such a measure. Also from
these reasons, the Bundeskartellamt has examined the topic of "encryption" not only from a security point of view but also with regard to an independent legal analysis.

Finally, encryption is also an example of the wide-ranging **information deficiencies** consumers face in a tech-based industry such as messenger and video services, which need to be addressed by the authorities involved in order to achieve sustainable improvements in consumer protection.

In 2020, when the first considerations regarding the sector enquiry into messenger and video services arose, the Bundeskartellamt carried out **research using a random sample of** around 40 messenger services[202] to find out how consumers are informed by the services about security aspects, especially encryption. At that time, a confusing and unclear picture emerged. Almost all messenger services had published information on company-related security standards on their websites. In some cases, the information was presented transparently and was understandable, but in others it was hard to penetrate. The majority of messenger services had their own sections on the topic of security on their homepages. These then contained information on the encryption procedure in varying depth. In some cases, there were further links under the corresponding heading leading to further information. It was noticeable that most of the services only provided keywords whose concrete content could not be directly inferred. For example, services had advertised "secure or strong encryption". Only with further research or by reading the data protection guidelines did the type and degree of encryption, for example, become clear. In this context, there were also occasional non-transparent references. Particularly in the case of the information provided by leading messenger services, it was not always clear when the information only referred to the

[202] The services included in the sample did not fully correspond to the subsequent addressees or the services that answered the questionnaire.

The information was often not separated from specific information on the security of the communication, which made the flow of information more difficult. In addition, general data protection information was often not separated from specific information on the security of the communication, which made the flow of information more difficult. For example, in the case of messenger services from individual operating system manufacturers, information could only be obtained from the privacy policy. In some cases, the information provided by individual services was also contradictory for the reader. Nevertheless, there were also positive examples. For example, some services provided concrete information and explanations of technical terms or listed setting options. Various fact sheets or well-designed FAQ sections made it easier to find information. In addition, there were separate explanatory videos or instructions on how to make the personal profile more secure.
Due to the diverging results, which did not allow for a clear assessment, the Bundeskartellamt left possible violations of unfair competition law - disregard of the transparency requirement pursuant to Section 5a UWG - in the scope of the investigation.

aa) Principles of fair trading law

Messenger and video services must inform consumers in accordance with the rules of the UWG. Relevant in this context is Section 5a (1) UWG, according to which it is misleading if consumers are deprived of material information that is needed for an informed decision and the deprivation of which is likely to induce a business decision that would not otherwise have been taken. Section 5a (1) UWG consequently creates a duty of transparency for material information.[203] A breach of the duty of transparency may exist in the present case if users are not adequately informed about **security-relevant aspects of** a messenger or video service.

bb) Failure to comply with fair trading law

There is a good year between the Bundeskartellamt's research on encryption and the return of the results of the investigations. Technical development has progressed during this time. As the BSI already stated in its publication in November 2021, end-to-end encryption is considered state of the art. The scandal surrounding the special and technically incorrect interpretation of end-to-end encryption at a video conference provider has since been clarified. The end point of the communication was not the users themselves - as was the case.

[203] *Dreher/Kulka* Competition and Cartel Law § 3 marginal no. 383.

end-to-end encryption - but the systems involved (see also Chapter D.I.4.a) cc)). In the case of videoconferencing, this cannot be the devices of the users among themselves, but the device of each user with the server of the service used, which corresponds to transport encryption.[204] Due to the public criticism triggered by this in the press and the subsequent improvements which were also publicly reported, the Bundeskartellamt assumes that the answer to the questionnaire was based on the correct definition of end-to-end encryption, unless this can be concluded anyway from the explanations provided by the respondents.

The services surveyed answered the Bundeskartellamt's questionnaire on encryption and especially end-to-end encryption in detail for the most part. Video conferencing providers referred to the technical limitations that do not allow end-to-end encryption, e.g. for webinars with very many participants or when using certain functions. These **functions in videoconferencing** include, for example, dial-in from the public telephone network or the recording of meetings by the service providing the service, as well as the connection of certain external devices (e.g. room conferencing system devices based on the SIP-

protocol based) or the use of "assistants". The high **effort involved in the encryption of group chats** is also reflected in the survey results. Only five services have stated that they equip all their functions with end-to-end encryption (see again chapter D.I.4.a) and b)).

For a violation of the duty of transparency under unfair competition law, it would have to be proven in this context whether information on the security of the communication, such as the use of a special encryption method, is to be assessed as material within the meaning of Section 5a (1) UWG, whether the withheld information is necessary for making an informed business decision and whether it can be suitable to influence the decision of the users of a messenger and video service in such a way that they might have decided differently if the relevant facts had been disclosed. The **legal risks that arise for messenger** and video services in relation to their **information practices on the subject of privacy are** outlined below.

---

[204] See also, for example, *datenschutz notizen*, https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-videokonferenzen-1825597 and *The Intercept,* Zoom meetings aren't end-to-end encrypted, despite misleading marketing, 31 March 2020, available at: https://theintercept.com/2020/03/31/zoom-meeting-encryption/ and *Golem*, Zoom advertises end-to-end encryption - which doesn't exist, cf. https://www.golem.de/news/homeoffice-neue-sicherheitsluecken-in-zoom-entdeckt-2004-147670-2.html.

safety-relevant properties. A conclusive assessment cannot be made; it ultimately requires clarification in the specific case.

First of all, for the **materiality of** information required by Section 5a (1) UWG, it must be questioned whether the consumer can at all expect to receive information on the security of communication through end-to-end encryption. The use of messenger and video services naturally involves the processing of personal data. Their protection and secure handling is a declared goal of data protection law. Moreover, during the registration process, users are usually asked to accept the specific data protection and usage conditions. Thus, consumers can and may assume that they will receive information on the security of their data. In the second step, it depends on whether the missing information is important for the consumer's decision.[205] Here, the interests of the services, such as the time and cost involved or existing confidentiality concerns, must now also be taken into account as part of a balancing of interests.[206] The focus is on the **reasonableness of obtaining information for** the service.[207] It is given in any case if the provision of the information meets the standard of expertise and diligence and it can be assumed that the services provide the information to the users in accordance with decent market practices and the principle of good faith.[208] According to the results of the investigations, the services publicly provide extensive information on general data security, partly also on encryption and end-to-end encryption, albeit in different ways and quality. The services have for the most part disclosed the publicly accessible sources on the internet to the Bundeskartellamt in response to a corresponding request in the questionnaire. Some of them advertise their high security standards, including encryption. From this point of view, there is much to be said for the fact that this is **essential information.**

The fact that consumers are "**deprived**" of essential information on data security, in particular on end-to-end encryption, by the service within the meaning of Section 5a (1) UWG can be measured in the present context above all by whether the information is provided according to

§ Section 5a (2) no. 2 UWG merely provided in **an unclear, incomprehensible or ambiguous manner.**

---

[205] *MüKo-UWG/Alexander* § 5a marginal no. 223.

[206] BGH, Judgment of 21.07.2016 - I ZR 26/15 "*LGA tested*" para. 33.

[207] *Köhler/Bornkamm/Feddersen/Köhler* UWG § 5a marginal no. 3.15.

[208] Cf. ECJ, Judgment of 07.06.2016 - C-310/15 "*Deroo-Blanquart*" para. 33f.

become. In particular, information is incomprehensible if the average consumer does not understand its meaning or significance. Technical terms or special abbreviations are relevant in the context.[209] It also includes cases where a service uses different font sizes or even languages for different information, making the information so impenetrable and incomprehensible and thus ultimately useless for consumers. The design of the website and the methods of information provision described could therefore also be decisive for the information obligation of messenger and video services. Although almost half of the services investigated have corresponding sections on their websites, these usually refer to the general provisions or general FAQs or the respective support centre. Consumers can only find keywords on the homepage as well as under the heading "Security". These are then written in understandable language and explained with sketches, but more in-depth information about consequences, restrictions or special cases cannot be found at this point. If concrete information is sought, it is usually necessary to read the data protection regulations. In most cases, however, these are then formulated in English. In particular, non-transparent references or redirections to other websites could be of importance for an offence of **withholding.**

In the present case, however, there could be no **reason for a** breach of **the** duty of transparency under Section 5a (1) No. 2 UWG, as the market development is far advanced, end-to-end encryption is considered state of the art and is used throughout the industry (even if it is remarkable against this background that some well-known services do not yet implement it). However, if end-to-end encryption is so widespread, it may not make a significant difference from the consumer's perspective, at least in terms of this security feature, which service they register with. However, it is not possible to reliably predict consumer behaviour as precisely as possible with regard to the use and selection of messenger services depending on the encryption standard, as has already been made clear at various points in this report. If necessary, a corresponding consumer survey would have to be carried out, which, however, only seems legitimate within the framework of a sector enquiry if chances of clarification could be expected. But even that is likely to be uncertain. The term "encryption" alone is open to interpretation. The distinction between the different variants of transport encryption and end-to-end encryption is not clear.

[209] *Köhler/Bornkamm/Feddersen/Köhler* UWG § 5a marginal no. 3.30.

Encryption requires expertise that cannot be assumed among consumers.

A certain significance for the assessment of business relevance should therefore be attributed to the **classification of consumer behaviour from the company's point of view.** Information on how the individual messenger and video services bind their users to their own service could be helpful for this. In particular, it would provide information on the reasons why users decide to use the respective service. The Bundeskartellamt questioned the services accordingly in its investigations. The majority of the industry players interviewed had stated that they were valued, among other things, for the high level of data protection or data security. However, this is contradictory or at least not in line with other investigation results: The Bundeskartellamt had asked the messenger and video services for information on where users are informed about encryption. 60% of the services named the website / internet address whose weaknesses in the transmission of information had already been described. Only one in nine services provided additional information on encryption methods. Approximately one third of the services stated that there is no information on encryption for users.

The Bundeskartellamt has also asked the industry to describe whether **encryption against payment** can be further improved. In the aforementioned research preceding the investigations, product differentiation depending on the encryption standard was only evident in a few individual services. During the investigations, it also became clear that the vast majority of services do not offer additional encryption for a fee. One service surveyed enables the encryption of dormant data for business customers for a fee. Customers could also revoke encryption at various levels. Only one other service said it offered more extensive control over encryption procedures, but end-to-end encryption was basically included in the subscription regardless.

The fact that the services stated that they were selected because of their data security, but then do **not** offer **better encryption for** a **fee,** may be explained by strategic response behaviour in the context of a consumer law investigation. However, it could also be due to the fact that there are still many free offers, i.e. without a regular fee for using the app.

Ultimately, a transparency violation will not be easily justified by information deficiencies regarding the type of encryption. Even if security features can be counted among the essential information, their commercial relevance is likely to be limited as a result of the

market development towards end-to-end encryption as an industry standard and due to the consumer perspective, which cannot be assessed without further investigative effort, will be difficult to justify.

5. Conclusion - a checklist for "home use

The data security of messenger and video services is not determined solely by individual security aspects, such as the type and extent of encryption. Rather, it is a matter of the interplay of various criteria, which in themselves do not yet allow a statement about data protection friendliness.
For outsiders, the analysis is made more difficult by the fact that different facets are conceivable for many criteria and an assessment must take this complexity into account. For example, a closed messaging system with proprietary, i.e. not open source code, should not be readily suspected of harbouring privacy issues. Services with a proprietary source code can increase **trust in the implementation** if independent security audits, certifications according to ISO 27001 are carried out or the cryptographic design criteria are published, which is also practised by some services.[210]
Another example of the complexity of an assessment is end-to-end encryption. The **technical limitations and prerequisites as** well as the often practised **implementation as an option that** users have to set leave non-expert outsiders in the dark as to the concrete data protection quality of the various services in this question.
While consumers can hardly check and evaluate the specific characteristics of the security criteria of messenger and video services, it seems feasible for them to at least ascertain the existence of the individual security measures and to keep a quasi "checklist" (Figure 13). **Clear, consumer-oriented communication by** the services on what is practised, what is already preset and where options exist as well as what is not possible would be helpful and desirable.
As relevant criteria for data security, the BSI has particularly emphasised **state-of-the-art protocol and encryption** (e.g. the double ratchet protocol), **compliance with international standards** and a **viewable source code.** Consumers need to think about the technical limitations of end-to-end encryption when they read the details of the

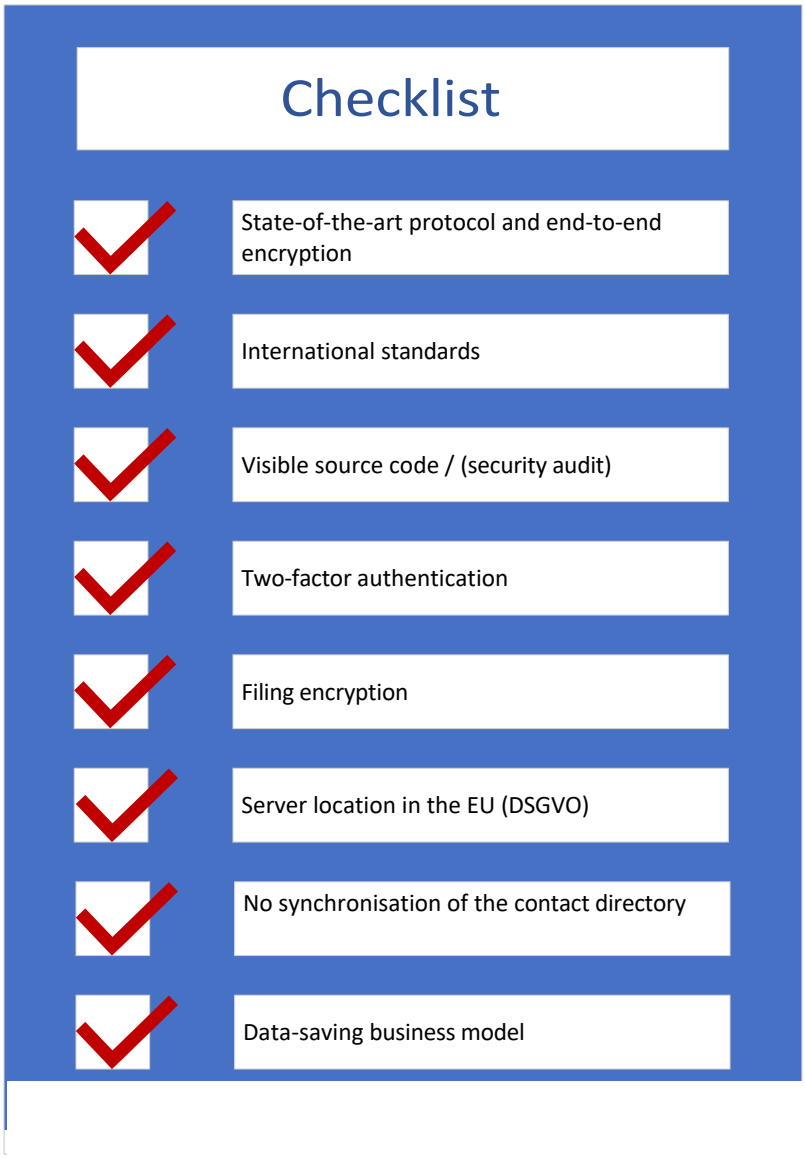
[210] Cf. *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

Check services for this. If international standards are adhered to and not individualised, the requirements for interoperability are also easier to fulfil. This point is therefore particularly important for possible gatekeepers in the sense of the DMA or interested applicant messenger and video services. Visibility of the source code is unlikely to be an advantage for the majority of consumers, as considerable expertise is required to assess it. Instead, some at least have security audits carried out by renowned institutions and publish them. Admittedly, these are not considered an equivalent substitute for visibility from a technical point of view. For interested consumers, however, the corresponding published ratings or seals of approval could be much easier to understand and thus an indication of the privacy-friendliness of the service. If the source code is open and can be rated, these ratings should also be communicated to consumers in an understandable way. Otherwise, they will not be able to use the information.

Other pillars of a security network are **two-factor authentication** and **file encryption**.[211] Both procedures are also practised in other areas (e.g. two-factor authentication in online banking or storage encryption on the home computer) and should be comprehensible for interested consumers.

[211] Cf. *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

Among the criteria for economical data processing, the **server location** with its implications for data protection legislation and legally compliant data storage should be emphasised first. Thus, data of European users should also be stored in the European Union.



Another point is the synchronisation of the contact directory, which should be dispensed with. From a data protection perspective, the legally compliant handling of users' **contacts is** essential for the quality of data protection, since users decide here not only about their own data, but also about the data of third parties. The reference to the privacy statement as the place where consumers can read about how the services handle their data is correct, but it is not sufficient because consumers do not pay attention to it for the various reasons mentioned. Furthermore

the **business model of** a messenger and video service can be considered the first indication of the **intensity of data sharing.**

Messenger and video services are an industry that generates technological and digital developments and innovations, especially on the part of the larger participants. Competing services are characterised by innovative business models and specialisations based on particular services and functions. Not only on the side of the free systems and applications is there a **lot of expertise and commitment in terms of independence and protection of** users' **personal data.** However, at the same time in the industry - as shown

- to find fault with various practices. The results of the sector enquiry suggest that various services do not use the expertise and possibilities in data protection and data security as would be desirable and technically possible from the users' point of view.

From the consumer's point of view, however, this is difficult to pin down to individual groups of services. According to the results of the investigation, **free messaging systems** and **open source services,** for example, score well on many of the criteria. However, the question of how data security is designed in detail ultimately depends on the selected server operator. The same applies to open source services when they are integrated into existing clients. Here, too, the service provider has many options for designing data security.

In general, users have **many choices** when it comes to messaging and videoconferencing, some of which require a certain awareness of security-related actions, such as the selection of the server operator just mentioned or the options for end-to-end encryption. Conversely, if consumers are willing to inform themselves, they can find a **wide range of options** to design their messenger or find the client that best meets their requirements and the chosen service is also future-proof in terms of interoperability due to data economy and the use of international standards.

Video conferencing services also offer their users many options. To a large extent, this is due to the orientation towards the wishes of business customers. A **high level of security** can be provided, especially for services that are mainly aimed at business customers. Ultimately, however, security-conscious action is often the **responsibility of the respective host** or administrator, regardless of whether this role is performed for business or private purposes.

As far as the practices to be criticised or the lack of commitment are concerned, this concerns, on the one hand, **encryption**. Individual messenger and video services that are popular with consumers

consumers are popular, and individual well-known video services also surprise with the fact that they do **not** implement state-of-the-art security and leave it at transport encryption, for example, or only use end-to-end encryption for certain functions, which cannot be justified with technical restrictions. Furthermore, it would be desirable that other security procedures, such as encryption of data on the end device, filing encryption, two-factor authentication as well as backups would have a higher degree of diffusion in the industry.

On the other hand, reference should be made to the legal analysis. Some services store **data in other European countries** or the exact storage location remains unclear. The **synchronisation of the contact directory as a** result of which third party data is processed illegally is also operated by various services. If users have to create **accounts,** as is the case with services of large corporations that operate a digital ecosystem, a lot of data is already collected through this.

It should be noted that the evaluation of data protection practices for consumers remains difficult and complex.

E. Data portability as a transition to interoperability?

With Article 20 (1) of the GDPR, the legislator has given consumers the right to receive personal data concerning them that has been provided to a controller in a structured, common and machine-readable format or to have it transferred directly to the new controller. Among experts, data portability and interoperability are often discussed in the same context.[212] It is questionable whether the conception of the standard can fundamentally capture the needs of the users of messenger and video services (see I.). There are also doubts about the practical significance of the provision for users when they want to change their messenger and video service, and thus also about the legal benefit for possible interoperability measures that go beyond this (see II.). Finally, as part of the investigations, the Bundeskartellamt asked the messenger and video services about the theoretical possibilities and the actual use of the transfer of stored personal data pursuant to Art. 20 GDPR (see III.).

I. Classification and claim of the provision

Pursuant to Article 20(1) of the GDPR, consumers may receive personal data concerning them which has been provided to a controller in a structured, commonly used and machine-readable format or have it transferred directly to the new controller. The consumer thus has the possibility to transfer these data to another controller without hindrance by the controller to whom the personal data were provided. The core of the provision is thus not only availability but also the **portability of personal data**, which is also referred to as data portability.

The origin of the norm and thus its affiliation to data protection law is partly disputed.[213] Some argue that it is a regulation with purely consumer protection and data protection implications.

---

[212] See for example *OECD* (2020): Consumer data rights and competition- background note, available at: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD (20 20)59 &docLanguage=En; *Yoo* (2020): Unpacking data portability, *CPI* antitrust chronicle November 2020, available at: https://www.competitionpolicyinternational.com/unpacking-data-portability/; *Kerber, Gil (*2020): Data portability rights: Limits, opportunities and the need for going beyond the portability of personal data, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715357.

[213] *Kühling/Buchner/Herbst,* DSGVO, Art. 20 marginal no. 4.

competition law objectives instead of data protection law objectives.[214] According to the prevailing opinion, however, the right to data portability is just as much a creative right as other data subjects' rights.[215] The decisive factor in the systematic classification is that the norm also pursues other objectives, in particular competition and internal market policy objectives, in addition to purely data protection objectives. Thus, the law strengthens the self-determination of consumers and at the same time promotes competition between the providers of social networks.[216] The provision is thus apparently not only intended to enable consumers to obtain their data. It is also intended to entitle them to dispose of it in a certain way freely and self-determined. In addition to the consequence that so-called "lock-in effects" can be prevented, the legislator hopes - as already indicated - for an increase in competition with regard to new innovation possibilities and the exchange of personal data.[217] Thus, although the origin of the provision is less based on classic data protection law
i. However, due to the consumer protection and market regulation aspects, it contributes to the overarching protective purpose of data protection law.[218]

II. Practical significance

The right to data portability according to Art. 20 (1) GDPR initially gives consumers far-reaching powers of disposition in dealing with their personal data. The right gains its significance not only through the general possibility of requesting one's data, but above all through the possibility standardised in Art. 20 (2) GDPR of having one's data transferred directly to a new data controller. In addition to the mere receipt of data, the possibility of direct transfer could facilitate switching projects, especially when investigating messenger services.

---

[214] *Dehmel/Hullen,* ZD 2013, 147, p. 153.

[215] Kühling/Buchner/Herbst*,* DSGVO, Art. 20 marginal no. 4.

[216] *Ehmann/Selmayr/Kamann/Braun,* DS-GVO, Art. 20 marginal no. 3.

[217] Article 29 Working Party, Guidelines on the Right to Data Portability, WP 242 rev.01 p. 6.

[218] *Kühling/Martin*, EuZW 2016, 448 pp. In concrete terms, the data protection character can furthermore be seen in the fact that the norm represents an expression of the European fundamental rights to private life and the protection of personal data, cf. *Auernhammer/Schürnmann* DS- GVO Art. 20 marginal no. 3. Due to the need for ever more modernisation of the law, Art. 20 GDPR can also be seen as an element of innovative fundamental rights in the digital age and thus as an expression of the further development of the law, cf. *Ehmann/Selmayr/Kamann/Braun GDPR Art. 20 marginal* no. 4; *Auernhammer/Schürnmann GDPR* Art. 20 marginal no. 3.

However, the concept of data portability may not reflect the essence of real-time exchange. "messaging" or "chat" and therefore already falls short of interoperability in its approach. back. Art. 12 (3) of the GDPR provides that the provision of the personal data "without delay, and in any case within one month of receipt of the application". Under certain circumstances, even an extension of two further months is possible. This suggests that **a transfer "in real time" is** neither desired nor possible on the basis of this standard. Even if data portability had to be guaranteed without any delay and every user could always switch back and forth between services immediately and at will, an exchange in real time, as is usual in messaging, would not come about. With regard to the facts of Article 20 of the GDPR, it should also be noted that the technical compatibility required for functioning interoperability cannot be mutually enforced. The data to be transferred must relate to the data subject and must have been provided by the data subject. In addition, conventional data processing must be automated pursuant to Art. 20 (1) (b) of the GDPR and must be based on one of the legal bases mentioned in Art. 20 (1) (a) of the GDPR. At the same time, however, the GDPR only imposes limited requirements on the technical format in which this data must be provided. Thus, recital 68 of the GDPR states that there is no obligation for the controller to "adopt or maintain technically compatible data processing systems". This restriction is to be understood in such a way that a direct transfer of data by the controller to another controller within the meaning of Article 20 (2) of the GDPR should take place, but if this is not technically feasible, this does not result in an obligation for the controller to make this possible.[219] In this case, Art. 20 GDPR does not oblige providers to create compatible data processing systems, which would, however, be a prerequisite for interoperability.

Probably the most significant problem from a data protection perspective is the lack of possibility to separate data in general. In addition to the so-called master data, the use of OTT services such as messenger and video services mainly involves data that also relate to other, third parties. An exclusion of such **third party data is** likely to miss the norm's purpose of creating far-reaching switching incentives to a great extent. In the meantime, there is agreement that under the premise of not violating the rights and freedoms of those third parties, they can also be part of the transmission claim. Consequently, there must be a corresponding legal basis for the data transfer. This is likely to be the case in particular in the case of OTT service use.

[219] See *Article 29 Working Party*, Guidelines on the right to data portability, WP 242 rev. 01, April 2017, p. 19.

This can probably be justified by the legitimate interest of the responsible party according to Art. 6 Para. 1 lit. f. DSGVO. Therefore, registration data, the profile picture, even if it depicts another person, and the contact directory are likely to be transferred.

A final difficulty is likely to lie in the **practical implementation of** the claim to data portability and thus also its usability for interoperability measures. Essential to this assessment is the requirement of making data available. What matters here is that the data subject himself has knowingly and actively disposed of his data. In practice, when users change providers, they will want to take their complete data with them, especially the content of exchanges via text messages - **chat histories.** Especially with regard to portable data, this can be difficult. For example, so-called observed data, i.e. data obtained by passively observing user behaviour, is not part of the claim. Also excluded is information based on an evaluation of provided data. In this context, the classification of chat histories is likely to play a major role. The decisive problem is that these are composed of data published by various chat participants. They have not been provided exclusively by the claimant. The individual messages published by them would have to be separated from the respective responses, which may be technically feasible, but would probably represent a disproportionate effort.

Against the background of the difficulties described above, it has not yet been possible to check whether consumers actually make use of this right. The Bundeskartellamt therefore asked the messenger and video services to what extent the legal claims were perceived by consumers and carried out by the messenger services. The corresponding information may also be relevant for the evaluation of possible interoperability projects. It could not only provide information about preferences and the (switching) behaviour of consumers, but also draw an up-to-date picture of the competitive situation (see below).

III. Investigation results

The Bundeskartellamt asked the messenger and video services about both the theoretical possibilities and the actual use of the transmission of stored personal data pursuant to Art. 20 GDPR.

In response to the question of how users can request the transfer of stored personal data from the respective service, almost all industry participants surveyed provided information. Some services provided an email address, some also provided a link to a download or web form. Whether and in which

However, the extent to which a data transfer pursuant to Art. 20 GDPR can actually be requested via these channels could not be verified in individual cases within the scope of the sector enquiry.
In addition, the Bundeskartellamt asked the industry what personal data users receive when they make a corresponding request. Of the services that provided information on the transmission of data, all transmit personal data, such as the user's first and last name, user name, age or gender. Only about half of the services also transmit data on devices/configuration, contacts/addresses, group memberships or app settings. Other **data transmitted by** the companies and apps included meeting data, (offline) messages, privacy settings, chat history, saved files, login data, public keys, usage data, ratings, rankings, stories, friends and histories. Some free messenger services have pointed out that it depends on the respective server what data is transmitted and how it can be transmitted to another service if necessary. Due to the server-related nature of these services, data transfer between different clients is not possible.
Generally not required.
Another question was about the **volume of requests made**, the processing and the transfer of data to a new provider. Only very few companies provided information on the number of applications or processed applications for data transfer in the last three years. The figures given ranged from 0 to around 300,000 applications per year. The number of applications was negligible in relation to the number of registered users of the respective service.
None of the services surveyed indicated that data was **transferred** directly to a **new provider** as a result of a request. However, some services indicated that the transfer of data to a third party provider is or can be done by the user themselves, so no further information is available on this. With regard to the **duration of the** processing of a request for data transfer, the services surveyed mentioned very different periods of time - between a few seconds and less than 1 month.
Finally, the services should describe where users are **informed** about their rights to data portability according to Art. 20 GDPR. The vast majority of the services surveyed provided corresponding information. However, the form and extent to which the required information is actually available under the aforementioned links could not be verified or evaluated in the context of the sector enquiry. Six of the services surveyed stated that they did not provide any corresponding information.

F. More data protection through interoperability?

Interoperability is a dynamically evolving concept, which is often adapted to different uses and had not yet been clearly defined for competition and consumer protection at the beginning of the sector enquiry into messenger and video services.[220] As a preliminary definition for the purposes of this sector enquiry, the Bundeskartellamt had **understood interoperability as** the **ability of independent, heterogeneous systems or products to cooperate to varying degrees**. From the consumer's point of view, interoperability refers to the ability to communicate with users of a messenger and video service other than one's own without having installed or registered for that other service. [221]

With the present sector enquiry, the Bundeskartellamt is taking up the subject of interoperability not only because it is an influencing factor for the environment of messenger and video services. The main question is whether **a better level of data protection can be achieved through interoperability**. The leading questions are, firstly, whether there is a direct effect. Behind this is the frequently expressed expectation that if the services were accessible to each other, consumers would no longer be afraid to switch messenger and video services because they would no longer be excluded from their previous contacts. In order to achieve the desired positive, direct effects on the level of data protection, consumers would need to

---

[220] Cf. e.g. For example, the definition used by the International Standards Organisation (ISO) in the field of cloud computing, cited in: *Brown,* Interoperability as a tool for competition regulation, *Preprint*, 30.07.2020, p. 32, available at: https://osf.io/preprints/lawarxiv/fbvxd/, and *Kerber/Schweitzer,* Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, pp. 39-58, para. 5, or *Palfrey/Gasser,* Interop*,* 2012, p. 5, so cited in: *Kerber/Schweitzer,* Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, pp. 39-58, para. 5.

[221] Closely related to interoperability is the term compatibility. However, the relationship to interoperability is not described uniformly. In some cases, compatibility is seen as a preliminary stage and necessary prerequisite for interoperability. If products are compatible, they can be used in parallel on a computer without software conflicts, for example. In the case of interoperability, they must also be able to work together or function. In some cases, interoperability is seen as a subcategory of compatibility, cf. *Kerber/Schweitzer,* Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, pp. 39-58, para. 5. In the theoretical economic literature, the term compatibility is usually used, whereas in interoperability has become established as a "buzzword" in information technology writings, without this The distinction between the two would be based on model-theoretical differences.

However, they should turn to privacy-friendly messenger and video services. According to the results of various consumer surveys, doubts about this seem quite justified (cf. F.II). But there are also indirect effects on the level of data protection through interoperability. The **negative effects of interoperability on competition and innovation** can also have consequences for data protection issues via data security.

For a better assessment of the guiding questions, a legal, scientific and conceptual classification will first be made in the following (see I.) It is interesting to see to what extent interoperability has already found its way into legal regulations at national and European level and what the reasons are for this. Particular reference should be made here to the Digital Markets Act, which in the meantime - after publication of the interim report on this sector enquiry

- has been finally discussed between the EU Commission, the EU Parliament and the EU Council of Ministers and has entered into force. Subsequently, it must be examined to what extent previous scientific findings can clarify the interrelationships between interoperability, innovation and competition or provide indications for problem solving and recommendations for action. Are they at all suitable for illuminating the complex interrelationships? Then it will be clarified how interoperability can be implemented organisationally and technically and how the corresponding regulations of the Digital Markets Act can be classified.

Subsequently, the focus is on consumers and their behaviour, which is difficult to predict. Will they fulfil the hopes placed in them by politicians and data protectionists or do they themselves have completely different wishes (see II.)?

Against this background, the results of the investigations into questions of interoperability are then presented, which were posed to the messenger and video services even before the inclusion of the interoperability regime in the drafts of the Digital Markets Act (see III.). The chapter concludes with conclusions that result from the interplay of investigation results and the DMA regulations. What impact on the level of data protection can be expected? As technical specifications and general conditions of reference offers according to the DMA of possible gatekeepers were not yet known at the time of publication of this report, only some basic comments can be made from a consumer law perspective (see IV.).

I. Interoperability - a conceptual, legal and scientific classification

1. Interoperability in competition and sector law

The Bundeskartellamt has initiated the consumer sector enquiry into messenger and video services under Section 32e (5) ARC; it is directed at messenger and video services as a sector of the economy and is therefore not directed against individual companies. An obligation to

In the Bundeskartellamt's view, interoperability cannot be derived from traditional consumer law. Only German commercial law has so far contained provisions which provide for an obligation to interoperate with competing services to be imposed by the authorities (under strict conditions and in a specific procedure), namely Section 19a (2) sentence 1 no. 5 of the Act against Restraints of Competition (GWB) and Section 21 (2) of the Telecommunications Act (TKG).[222]

With the inclusion of an interoperability obligation in the drafts of the Digital Markets Act in March 2022, the legal environment of messenger and video services in terms of interoperability has become more concrete. Due to the ongoing legal-political discussion on a legal obligation of messenger and video services for horizontal interoperability, the Bundeskartellamt had already asked the companies surveyed questions on this complex of topics in its investigation before the agreement in the trilogue on the DMA in March 2022. In their answers to the Bundeskartellamt's questionnaire, individual messenger and video services had referred to the legal framework applicable in 2021 for a possible mandatory interoperability measure. These are Section 19a GWB (see a) below) and Article 61 (2) subparagraph 1 lit. c of the European Electronic Communications Code[223] (see b) below), which has found its way into Section 21 (2) TKG. Therefore, these provisions will be briefly mentioned here. For a detailed discussion, please refer to the relevant specialist literature.[224] The Digital Markets Act will now supplement the legal framework and could have far-reaching effects for some messenger and video services (see c) below).

a) § Section 19a Act against Restraints of Competition (GWB)

Pursuant to Section 19a (1) of the ARC, the Bundeskartellamt can determine that a company has an overriding importance for competition on the market and, based on this, prohibit certain conduct by the company pursuant to Section 19a (2) of the ARC. Unlike in the

[222] Art. 1 of the Act on the Implementation of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 on the European Electronic Communications Code (recast) and on the Modernisation of Telecommunications Law (Telecommunications Modernisation Act) of 23.06.2021, BGBL. I 1858 - TKG.

[223] Directive of the European Parliament and of the Council on the European Electronic Communications Code (EU) 2018/1972 of 11.12.2018, OJ L 321 of 17.12.2018, p. 36 - EKEK.

[224] Cf. for example the interdisciplinary consideration by *Gerpott*, Interoperability of messenger services and social networks of large online platforms, CR 2022, 133 ff, *Kühling/Hildebrandt/Bulowski*, Die Zukunft der Interoperablitätsregulierung für OTT-Kommunikationsdienste, K & R 2022, 670 ff.

classic abuse control, it is therefore not necessary to identify a dominant position for each individual case, which can speed up enforcement.

Pursuant to Section 19a (2) sentence 1 no. 5 GWB, the Bundeskartellamt can prohibit "refusing or impeding the interoperability of products or services or the portability of data and thus hindering competition". The explanatory memorandum to the Act states that measures directed against interoperability can secure and further consolidate strong market positions of the norm addressees of Section 19a GWB. They can favour lock-in effects.

With Section 19a GWB, German law - unlike the Digital Markets Act - does not in principle link to individual (types of) service(s), but allows the company as a whole and also cross-market interactions of services within a digital ecosystem to be taken into account.[225]

The explanatory memorandum also mentions the possible ambivalent effects of interoperability and "other possible disadvantages" of an interoperability obligation. Explicitly mentioned are network effects in favour of competitors of the norm addressee, which could be weakened, as well as the hindrance of innovation and product design possibilities and the possibility that the norm addressee could gain access to (even) more data.

b) European Electronic Communications Code (ECC) / Telecommunications Act (TKG)

The EKEK, which entered into force in December 2018, allows national regulatory authorities - in Germany the **Federal Network Agency (BNetzA)** - to **impose interoperability obligations on** providers of "number-independent interpersonal communications services" (Art. 61, para. 2 subpara. 1 lit. c. EKEK). Market dominance in accordance with Art. 68 Para. 3 lit. a DETEC is not a necessary prerequisite for this. However, an interoperability obligation can only be implemented under the conditions specified in Art. 61, para. 2, subpara. 2 FCA. In particular, interoperability may only be

[225] So far, the Bundeskartellamt has found that Alphabet (Google), Meta and Amazon are of overriding importance for the entire market, see BKartA, Beschl. v. 30.12.2021, Az. B7-61/21 "*Alphabet (Google)*"- Case Report v. 05.01.2022; BKartA, Beschl. v. 03.04.2023, Az. B9-67/21 "*Apple*" - case report v. 05.04.2023, BKartA, Beschl. v. 02.05.2022, Az. B6-27/21 "*Meta*" - case report v. 30.06.2022; BKartA, Beschl. 05.07.2022, Az. B2-55/21 "*Amazon*" - case report v. 06.07.2022, . See also *Bundeskartellamt*, Statement on the Public Hearing of the Economic Committee on the Digital Markets Act, 25 April 2022, available at: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf.

be imposed when **end-to-end connectivity between end-users is**
is at risk. The Code has been implemented in the TKG.
According to § 21 (2) TKG (new), in the event of a threat to end-to-end connectivity between end users, the Federal Network Agency can oblige providers of number-independent interpersonal telecommunications services - and thus also messenger services - to make their services interoperable. The Federal Network Agency currently assumes that end-to-end connectivity is currently ensured by the fact that end users can use number-based interpersonal telecommunications services, i.e., classic telecommunications services. "However, future technical developments and also the behaviour of users could lead to insufficient interoperability between
interpersonal telecommunications services"[226] .

c) Digital Markets Act

Together with the Digital Services Act (DSA for short), the law on digital services, which was passed on 1. The Digital Markets Act, which came into force on 1 November 2022, is one of the
core elements of the EU's digital strategy. [227]
With the two related regulations, the European Union wants to reorganise internet regulation and, in doing so, primarily address the power of large online platforms. The DMA is primarily aimed at competition issues, the DSA at other areas of platform regulation such as online advertising, liability issues or content moderation.[228]
The Digital Markets Act lays down **rules for** certain **large online platforms.** Regulatory measures are intended to protect commercial users as well as end users.

---

[226] *Bundesnetzagentur*, Interoperability between Messenger Services, November 2021, available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/Online Kom/diskussionspapier_IOP.pdf? blob=publicationFile&v=3.

[227] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065 and Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur- lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925.

[228] Cf. *Netzpolitik.org*, available at: https://netzpolitik.org/2021/plattformregulierung-europas-weg-in- die-digitale-zukunft/.

end-users of gatekeeper-provided core platform services across the European Union are protected from unfair gatekeeper practices.[229]

In autumn 2021, the EU Parliament, the EU Commission and the member states had started negotiations on the DSA proposal and the DMA proposal .[230]

In December 2021, the plenary of the European Parliament had adopted a common position on the DMA and defined its negotiating position. The European Parliament's **DMA draft** provided - in contrast to the EU Commission's draft - for a

Interoperability obligation for gatekeepers related to "number-independent interpersonal number-independent interpersonal communication services" ("number-independent interpersonal communication services", which includes messenger services). Interoperability already played a role in the EU Commission's DMA proposal. However, in contrast to Section 19a GWB, interoperability should be taken into account in particular in the vertical relationship between the market participants.

On 24 March 2022, **an agreement** was reached in **the trilogue,** i.e. between representatives of the EU Commission, the EU Parliament and the EU Council of Ministers. According to this, the gatekeeper must provide the necessary technical interfaces or comparable solutions at the request of another messenger service or market newcomer in order to enable interoperability without imposing costs. The provision refers to an interoperability of **basic functions - text messages first -** including the level of security guaranteed by the gatekeeper to its own users (including end-to-end encryption). Compared to the previous draft, the catalogue of basic functions has been extended to include the sharing of any files, not only pictures, voice messages and videos. Each gatekeeper is obliged to provide a **reference offer**

("reference offer"), which contains the essential technical details, the general terms and conditions and the contains necessary information on data security and end-to-end encryption. Requests for interoperability of bilateral text messages must be implemented within three months. For the **interoperability of other functions,** different deadlines are provided, after which a request for interoperability must be met at the earliest, namely for **group text messages** two years after the designation as gatekeeper of the respective messenger service and for **video calls** between two as well as more users four years after the designation as gatekeeper of the respective messenger service.

---

[229] Cf. DMA, recital 7, available at: https://data.consilium.europa.eu/doc/document/PE-17- 2022-INIT/en/pdf.

[230] *European Commission*, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), 15.12.2020, COM (2020) 842 final, 2020/0374(COD) - DMA Proposal.

Designation of the respective messenger service. The European Commission may exceptionally extend the above-mentioned deadlines, in particular if this is the only way to ensure end-to-end encryption. The European Commission shall also be empowered to adopt, by delegated act, the list of the The Commission has the power to amend the basic functionalities and to make "operational and technical arrangements" by means of implementing acts.

In its statement on the public hearing of the Economic Committee on the Digital Markets Act, the Bundeskartellamt welcomed the European legislative project. At the same time, it emphasised that in future an application of competition law complementing the DMA will also be necessary vis-à-vis the large digital companies and explained this in detail.[231]

It should be noted that competition and sector law is not the basis of the present consumer law sector enquiry. However, the German legislator had already attributed great importance to the topic of interoperability before the enactment of the Digital Markets Act and had mentioned its complexity in the existing legislation due to possible negative effects. This had supported the Bundeskartellamt's view that a survey of the industry could be a sound contribution to better assess the relationship between the effects of interoperability. First, the following chapter will describe the extent to which previous scientific findings can clarify the relationships between interoperability, innovation and competition or provide indications for problem solving and recommendations for action.

2. Contribution of scientific knowledge

The Bundeskartellamt is investigating what effects can be expected from a possible interoperability project on the level of data protection in messenger and video services. The Bundeskartellamt's focus is therefore on a specific section of the topic - **interoperability and data protection** - in which, however, there are certainly interactions with competition, innovation and data security. First, the complexity of the issue will be illustrated (see a)). Subsequently, essential insights into the theory of networks (see b)) and possible effects of interoperability on competition and innovation will be described.

---

[231] See for details *Bundeskartellamt*, Statement on the Public Hearing of the Economic Committee on the Digital Markets Act, 25 April 2022, available at: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf.

(see c)). Finally, there is a short summary of possible effects of standardisation processes (see d)).

a) Class instead of mass

The industry of messenger and video services, as defined for the purposes of the study, includes a wide variety of companies and applications: Concentration on just one function hardly exists any more. Instead, as seen, there are many business models and applications that combine both messaging, video conferencing, sometimes also social media functions or features for communication and collaboration. Some messenger services benefit from a large user base via network effects. Others are interoperable anyway, so that the number of users of the respective service is of little importance for its attractiveness in itself. The pricing of the services is also different. Some services are offered free of charge, others are financed through fees for basic or additional services. The price as an important parameter thus depends on completely different variables. For these reasons, not all theoretical scientific contributions are equally relevant for all industry participants. Translated into economic models, this means that **no uniform industry-wide model conditions** can be defined. Rather, model-based analyses therefore already face various **diagnostic difficulties.** The variety of dependencies and variables can only be mapped to a limited extent. Only selected parameters can be observed, for which certain market conditions must be set. But what is the initial situation? Does competition already exist? These questions are as complex as the object of analysis itself or the formulation of concrete recommendations for action.

One can also formulate it the other way round. A wide range of scientific findings that touch on the topics of the study in some way come into question. However, concrete indications for possible solutions cannot be derived without further ado.

The practical implementation of interoperability in particular was more prominent in analyses by foreign competition authorities than in purely scientific publications. In the investigations by the CMA (Competition and Markets Authority) and ACCC (Australian Competition & Consumer Commission), the dominance of Facebook and Google in particular was worked out in detail. However, the CMA's proposals mainly relate to social networks and less to messenger services. The ACCC does deal with messenger services, but does not consider interoperability issues. Accordingly, the conclusions are different: Whereas the Australian ACCC speaks of initiatives in favour of more

interoperability, the British CMA takes a much more positive view and makes concrete proposals for the area of social networks as to what an interoperability obligation could look like.[232] In the following, an overview will be given of **those explanatory approaches** that are comparatively closely related to the topic of the study or the industry participants.

b) Network theory

With the triumphal march of (social) networks and platforms, an intensive discussion has developed around the underlying scientific explanatory approaches - the economic theory of networks[233] . In the meantime, this discussion is not only taking place in the academic environment and among experts. The topic has also arrived in the general consumer public, as most recently vividly demonstrated by the report published by the Federation of German Consumer Organisations in 2021.[234]

Users of messenger and video services particularly appreciate those networks where they can reach many other users (so-called positive direct network effect).[235] Self-reinforcement effects can result from positive network effects: Large networks become increasingly attractive for users. However, depending on their strength, network effects can also contribute to a previously competitive market threatening to collapse at a certain concentration and the entire demand being concentrated on only one provider.

---

[232] See *Competition and Markets Authority* (2020), Online platforms and digital advertising - Market study final report, July 2020, p. 5, available at: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study and *Australian Competition & Consumer Commission:* Digital Platform Services Inquiry - Interim Report, September 2019, available at: https://www.accc.gov.au/focus- areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/final-report.

[233] See *Katz/Shapiro*, Network Externalities, Competition, and Compatibility, The American Economic Review, 1985, 75(3), pp. 424-440; *Farrell/Saloner*, Standardisation, Compatibility, and Innovation, The RAND Journal of Economics, 1985, 16(1), pp. 70-83.

[234] *Verbraucherzentrale Bundesverband* (2021), Interoperabiltiät bei Messenger-Diensten, 17 May 2021, available at: https://www.vzbv.de/sites/default/files/2021-05/21-05-18_vzbv__Diskussionspapier_Interoperabilit%C3%A4t_Messenger.pdf.

[235] For a classification from a competition law perspective, see e.g. *Bundeskartellamt*, Marktmacht von Plattformen und Netzwerken, Working Paper, June 2016, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf? blob =publicationFile&v=2.

while the other competitors do not reach the necessary critical size, so-called **tipping**.[236] Even a market that cannot yet be described as "tipped", but in which one provider nevertheless has by far the highest number of users, harbours the danger of strong ties to one network and high switching costs for users (**lock-in effects**).[237] For social networks - which are partly represented in the sector enquiry by their own messaging functions - proposals for possible interoperability obligations have therefore already been voiced. In its market study on internet platforms and digital advertising, the Competition and Markets Authority (CMA) argues in favour of obliging Facebook to more interoperability - within a limited framework.[238]

These dangers have led to an increased focus on an essential characteristic of such markets - a lack of interoperability. Interoperability is associated with the hope of dissolving or at least mitigating the pull of network effects in order to improve market structures.

In the following, insights into the relationship between interoperability, competition and innovation will be outlined.

c) Impact on competition and innovation

The effects of interoperability on competition[239] and innovation cannot be completely disregarded due to the aforementioned interaction, especially since intensive research is still being carried out on this topic today. The **competitive effects of** interoperability are described in

---

[236] Cf. *Bundeskartellamt*, B6-113/15, Working Paper - Market Power of Platforms and Networks, June 2016, p. 104 ff. with further references, available at: https://www.bundeskartellamt.de/SharedDocs/Publika tion/DE/Berichte/Think-Tank-Bericht.pdf?_blob=publicationFile&v=2.

[237] See *Autorité de la concurrence/Competition and Markets Authority,* The economics of open and closed systems, 2014, para. 2.20.

[238] Cf. *Competition and Markets Authority,* Online platforms and digital advertising, Market study, Final report, July 2020, para. 8.49 ff and Appendix W.

[239] Cf. e.g. *Belleflamme/Peitz*, Platforms and Network Effects, in: Corchon/Marini (eds.), Handbook of Game Theory and Industrial Organization, Vol. II, 2018, pp. 286-317, ch. 3.3 and *Crémer/Rey/Tirole*, Connectivity in the Commercial Internet, The Journal of Industrial Economics, 2000, 48(4), 433-472 as well as *Katz/Shapiro*, Network Externalities, Competition, and Compatibility, The American Economic Review, 1985, 75(3), pp. 424-440 or *Malueg/Schwartz,* Compatibility incentives of a large network facing multiple rivals, Journal of Industrial Economics, 2002, 54(4), pp. 527-567 and *Shy*, A Short Survey of Network Economics. Review of Industrial Organization, 2011, 38, pp. 119-149, ch. 3.1.

numerous theoretical and model-theoretical analyses. The result of the majority of the studies is firstly that interoperability leads to a shift from competition "for the market" to competition "in the market". Secondly, depending on the market structure and consumer behaviour, different effects on **consumer welfare are** to be expected. As far as innovation incentives are concerned, interoperability is again mostly associated with positive effects. However, this applies mainly to markets with homogeneous or standardised products.

In contrast, **digital markets** are characterised by a constant innovation development that does not follow any fixed rules.[240] A possible interoperability obligation is therefore likely to have a significant impact on innovative markets. Negative effects are increasingly cited here.

Interoperability requires that the various messenger and video services offer common functions so that users can exchange information with each other via the various communication channels (text messages, telephony, video telephony, etc.). This poses the risk that interoperable functions, once created, will not be sufficiently further developed. Competition for new innovative business models and **product differentiation** valued by the user could decline.

Depending on the exact form of an interoperability obligation, studies have shown that it is even to be feared that innovations of one company would have to be made available to all competitors. Usability and corresponding incentives to drive new developments would be impaired. The concept of interoperability is said to have gradations that mitigate these negative effects by making only **basic functions** interoperable. The theoretical claim of the proponents is that in this way differentiation possibilities and innovation incentives are preserved, at least for those functions that do not fall under the interoperability obligation.

Nevertheless, interoperability can also have **positive effects** on innovation activity in digital business fields. In science, this includes **lower market entry hurdles** and **reduced lock-in effects.** Positive effects could therefore also be expected for innovations in the area of complementary products. Incentives to innovate and opportunities for differentiation would increase if new products or services can build on the interoperable product.[241] The internet itself can be considered as an example, which for

---

[240] *Cremer/de Montjoye/Schweitzer*, Competition Policy for the digital era, Report for the EU Commission, 2019, p. 35, available at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

[241] *Kerber*, Data Sharing in IOT Ecosystems and Competition Law: the Example of Connected Cars, Journal of Competition Law & Economics, 2019, 15(4), pp. 381-426, Ch. II.B.

has provided an enormous boost to innovation in probably almost every sector of the economy. This has been achieved not least by the fact that the data can be transmitted in a wide variety of formats via the internet.[242]

Reduced innovation activity with the effects described above would also have an impact on the areas of **data security and data protection**, which are particularly relevant for messenger and video services. As far as the Bundeskartellamt is currently aware, there are no empirical results on this. There are a number of theoretical essays on the potential competition effects in the course of the introduction of the GDPR or on the effects of data portability and interoperability on the level of data protection, which the OECD has compiled in its publication "Consumer Data Rights and Competition - Background note"[243] . As was to be expected, the results, like the studies on the interactions with competition and innovation, do not point in a clear direction.

Scientific findings also exist on the effects of standardisation and various implementation questions and details in this context. Due to the mass of findings, the following section will only briefly refer to essential aspects for the messenger and video services sector.

d) Effects of standardisation

If interoperability is to be implemented technically, the participating systems must be designed in such a way that they comply with certain interoperable standards. Standardisations for the Internet, especially for the protocols, are - as already explained above - usually implemented by a standardisation organisation, the Internet Engineering Task Force (IETF), which publishes **open standards** at the end of a long discussion process.[244] Open standards means that each service will decide on the implementation of a standard according to its corporate strategy, which will probably depend on the nature and scope of the interoperability project.

---

[242] *Gasser,* Interoperability in the Digital Ecosystem, The Berkman Center for Internet and Society Research Publication No. 2015-13, 2015, ch. 3.1.

[243] Cf. *OECD* (2020): Consumer Data Rights and Competition - Background note, DAF/COMP(2020)1, available at: https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf.

[244] Cf. on other methods of standardisation *Farrell/Simcoe*, Four Paths to Compatibility, in: *Peitz/Waldfogel* (eds.), The Oxford Handbook of the Digital Economy, 2012, pp. 34-58, ch. 3.2.

Depending on the specific design of their development and implementation, as well as the characteristics of the markets concerned, economic experience has shown that standards can have beneficial and detrimental effects. In principle, standards can **reduce transaction costs, facilitate the market entry of new competitors and** contribute to **the diffusion of new technologies.** However, whether and to what extent an open standard becomes established depends largely on the quality of the technologies included in the standard and the adaptation costs of the actors who implement it. Adaptation **costs** arise when market participants have to comply with a mandatory standard that they have not used before or that they can only implement with considerable effort.[245]

Sustainable **welfare losses** are expected if an interoperable standard, once created, only allows incremental or no more innovations. Especially in the field of information technology, both the potential and the necessity for "radical" innovations are likely.

Innovations" exist. If network effects work in favour of an interoperable standard once it has been set, completely new technologies are likely to have a hard time breaking up these structures.[246] Quality competition is only possible within the set standards.

Uniform standards would **not necessarily** have to be **efficient or desirable.** In markets where there is effective competition, different services, products and services with varying degrees of interoperability may become established in the market.[247] Nevertheless, in many cases, standardisation of certain technologies or functions may be **an important goal of market participants,** either **for reasons of efficiency or individual merit**.

The extent to which standardisation brings opportunities or risks depends on the individual circumstances in an industry and the economic environment. When it comes to interoperability, it must be taken into account that this can be implemented and designed in many different ways, each of which is associated with advantages and disadvantages.

---

[245] For example, *Graef*, Mandating portability and interoperability in online social networks: regulatory and competition law issues in the European Union, Telecommunications Policy, 2015, 39 (6), pp. 502-514, chap.

4.2. in relation to social networks.

[246] *Gasser,* Interoperability in the Digital Ecosystem, The Berkman Center for Internet and Society Research Publication No. 2015-13, 2015, ch. 3.1.

[247] *Kerber/Schweitzer,* Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, pp. 39-58, para. 13.

3. Implementation and design

At the beginning of every interoperability project is the question of whether and to what extent measures should be taken by the sovereign. If this is desired, it is a matter of a **legal** interoperability obligation that is imposed on the companies concerned. The alternative is **voluntary** interoperability projects that can be initiated or promoted by the state, the industry as a whole or initiatives by individual market participants. From an **organisational point of view, there** are two ways to design an interoperability scheme. It can be implemented **symmetrically or asymmetrically.** While the symmetrical regulation affects all market participants, in the latter case only certain providers are obliged to make their services interoperable.[248]

In the messenger and video services industry, it was previously left to the market to produce interoperability regulations. This has changed with the enactment of the Digital Markets Act, which contains an asymmetric interoperability obligation. As described above, so-called gatekeepers among messenger and video services can be obliged to allow competitors access to their services.

As far as the **technical implementation is concerned**, only basic considerations that are necessary for understanding the industry's comments will be presented here.

Basic knowledge of the technical requirements and the effort involved is also helpful in creating an awareness of the efforts and costs involved. The way an interoperability scheme is implemented has a significant impact on the costs and effort involved, both technically and organisationally.

Details on the technical implementation of the Digital Markets Act are not yet known. Gatekeeper

[248] See *Kerber/Schweitzer,* Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, pp. 39-58, para. 6; *Choi/Whinston*, Benefits and requirements for interoperability in the electronic marketplace, Technology in Society, 2000, 22, pp. 33-44, 35 et seq.

are to provide an interface and ensure technical achievements such as end-to-end encryption.[249]
In principle, the technical implementation of interoperability essentially depends on the **linkage level** at which products or systems are to work together. In this study, the focus is on the substitutive technical linking of products or services. It is to be examined how interoperability can be established between different providers of the same "service type messenger and video service", which are in competition with each other. It is therefore not primarily a question of linking complementary services according to their functions. From the level of linkage, different technical possibilities can arise, which describe the **degree of interoperability.** For a linkage of two substitutive services, a so-called "full protocol interoperability" is required, as the European Commission states, for example. In contrast to the less strongly integrating and less
protocol interoperability", which is therefore mainly required for complementary products, a particularly high degree of interoperability. In addition, "data interoperability", on the basis of which data can be transmitted in real time, e.g. via programming interfaces (APIs), is also named.[250]
According to the Bundeskartellamt's findings, interoperability can in principle be implemented in several ways, which are accompanied by a varying intensity of technical interconnection: client interoperability, bridges and converters, etc., server interfaces and complete standardisation.
Client interoperability (multiprotocol clients) can make the exchange between messenger services more user-friendly. Client interoperability is already being practised in the industry in the form of the **multi-messenger services that** already exist. Multi-messengers provide a user interface through which consumers can read different messenger systems. Users must be registered with the respective services.

---

[249] In the study "Interoperability between Messaging Services - Secure Implementation of Encryption" presented by the *Federal Network Agency* on 3 May 2023, the authors Prof. Rösler and Prof. Schwenk present possible technical options in technical depth and discuss advantages and disadvantages as well as challenges, available at: https://www.bundesnetzagentur.de/DE/Fachhemen/Digitalisierung/Technologien/ Onlinekomm/Study_InteropEncryption.pdf? blob=publicationFile&v=1. The study includes seven messenger and video services and is based on an examination of publicly available technical documentation and scientific publications.

[250] Cf. *European Commission*, Final Report 2019, Competition policy for the digital era, p. 83 ff.

However, exchange is only possible within one system. If, for example, you want to send a reply to another messenger system, you have to do this via "copy and paste".[251] The technical prerequisite is that all participating services implement a public interface and disclose their own programming interface (API, see the following section) or protocol. The clients must implement the API of every other participating service (messaging system).

The most extensive form of interoperability can be established via **standardised server interfaces.** In general, connections to servers can be established via interfaces. **APIs (Application Programming Interface)** are used here for bilateral exchange. The API - also called programming interface - enables applications to communicate with each other. The API is not the database or even the server, but the code that regulates the access points for the server and enables communication.[252] More technical precautions have to be taken for this implementation variant than for the interoperability of the clients. If an **industry-wide standardised regime** were to be pursued, industry agreement would be needed to implement a standardised freely accessible messaging system or server API or protocol and to define sets of interoperable functions. Furthermore, all participating services would not only have to set up the interfaces and disclose their API or protocol, but also install **additional software** on their server or extend their own in order to communicate between the standard protocol and their own technology and to be able to deal with the users of other services. The service identifiers would also have to be integrated into the **uniform identifiers of** the interoperable system.

---

[251] Cf. *Open-Xchange* (2020): Whitepaper - A Technical and Policy Analysis of interoperable Internet Messaging, Version 1, September 2020.

[252] An API is a set of commands, functions, protocols and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so that codes do not have to be written from scratch. Cf. *Talend*, available at: https://www.talend.com/de/resources/was-ist-eine-api/. E.g. also proposed by Digitale Gesellschaft, Stellungnahme der *Digitalen Gesellschaft* e. V. zur Konsultation des Bundesministeriums der Justiz und für Verbraucherschutz zu Interoperabilität und Datenportabilität bei sozialen Netzwerken, May 2019, p. 4, available at: https://digitalegesellschaft.de/2019/05/stellungnahme-der-digitalen-gesellschaft-e-v-zur-konsultation-des-bundesministeriums-der-justiz-und-fuer- Verbraucherschutz-zu-interoperabilitaet-und-datenportabilitaet-bei-sozialen-netzwerken/.

be transferred. The clients would have less work to do. In any case, they would have to adopt the standard or the standardised protocol for the core function of message exchange.[253] Further standardisation would be necessary, for example, for incompatible encryption standards and for other functions, such as audio/video exchange, as different protocols are usually used here than for message exchange. With XMPP and Matrix, there are already free messenger systems with open standards.
For **consumers,** however, the focus is not on the technical requirements but on the functions that are made possible. In the case of messenger services, interoperability could be limited to **basic functions**, i.e. sending text messages and group chats, perhaps also the transfer of photos. A more far-reaching variant would provide that **all functions** offered by one messenger service can also be used by all other services.
The knowledge processes that must precede practical implementation are demanding and complex. After all, a key parameter that determines their success or failure is consumer behaviour. To what extent scepticism is still appropriate here with regard to data protection goals or whether hope can be raised, the following chapter will provide indications.

II. Consumer behaviour

Consumers are associated with high hopes and expectations in the discussion about interoperability and data protection. They are supposed to switch to privacy-friendly messenger and video services as soon as interoperability is established, since they can then reach their previous contacts even if they are not registered with the same service. The downside of this possible development is less frequently discussed, namely that it cannot be ruled out that the hoped-for incentives to switch will also decrease. If functions are largely standardised, no noticeable innovations are expected and network effects work across provider boundaries, consumers may not see why they should switch providers. If a certain **inertia in** the switching behaviour of consumers is still taken into account, it could theoretically not be ruled out that large services gain additional users through interoperability.[254]

---

[253] Cf. *Open-Xchange* (2020): Whitepaper - A Technical and Policy Analysis of interoperable Internet Messaging, Version 1, September 2020, p. 12.

[254] See also *Bitkom,* Position Paper, p. 5 f. for a similar argument.

Consumer behaviour is thus essential for the effectiveness of possible measures aimed at improving the level of data protection. However, it is not only unclear whether and to what extent consumers would benefit from interoperability in terms of improved data protection. It is already unclear whether they want interoperability at all.

Consumer surveys explicitly on this data protection-related topic are not known (more on this under 1.). Detached from any questions of interoperability, aspects of data protection have been the focus of consumer surveys more frequently in recent years. However, there has so far been a gap between the opinions and attitudes expressed by consumers and their practical implementation (cf. on this under 2.). It is therefore not surprising that so far there are no empirical findings that provide information on how consumers feel about interoperability and data protection.

1. Interoperability or multi-homing?

The Federal Network Agency conducted a consumer survey on online communication services in October / November 2019 and August 2021 respectively and published the results of the surveys in May 2020 and January 2022. The reports of the Federal Network Agency reveal the diversity of consumer behaviour in the use of OTT services .[255]

Users of messenger services can use several services in parallel without much effort (so-called **multi-homing**[256]). According to the results of the Federal Network Agency, in 2021 around 73% of all respondents used at least two different messenger services in parallel. This means that almost three quarters of respondents were already using multi-homing. In the survey in 2019, this proportion was still around two-thirds of respondents (68%), so that there is a clear increase here.

---

[255] Cf. *Bundesnetzagentur (2020)*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, available at: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte /2020/OTT.pdf? blob=publicationFile&v=6 and *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/Online Kom/befragung_kurz21.pdf? blob=publicationFile&v=3.

[256] The exact definition of this term is the subject of intense debate in competition law practice and is not interpreted uniformly. According to a narrow understanding, multi-homing can only be spoken of if there is a parallel use of the same demand. For a more in-depth discussion cf. e.g. *Bundeskartellamt*, Working Paper, Market Power of Platforms and Networks, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank- Bericht.pdf? blob=publicationFile&v=2.

increase can be observed. Multi-homing is generally more widespread among younger people than among older people. In the age group "up to 40 years", around 87% of respondents used at least two OTT communication services in 2021. On average, around four different services are even used in this age group. In the "over 40s" group, multi-homing is much less pronounced. Here, a good third of respondents (35%) used only one service in 2021; in 2019, however, this share was still at 46%.[257]
Some consumers seem to consciously separate different messenger services from each other in such a way that they are only accessible to certain people via certain channels.[258] For example, communication with good friends is conducted on other messenger services than exchanges in larger groups such as school classes or sports clubs. An obligation to interoperability would therefore possibly not be in the interest of these consumers - depending on the concrete design - due to these consumer preferences that are prioritised over the data protection aspect.
In contrast, a certain interest in interoperability could result from the fact that, according to the survey conducted by the Federal Network Agency in 2020, almost a third of OTT users already wanted to contact a person, but were unable to do so because that person did not use the same messenger service.[259] Accordingly, **positive direct network effects** seem to be particularly important in the use of OTT communication services. The more contacts of users can be reached via a certain service, the higher the interest tends to be in using exactly this service as well.
When asked directly about **interoperability**, however, no clear opinion emerges according to the current report of the Federal Network Agency. 43% of the OTT users surveyed think it is (rather) important that users of different services can communicate with each other, while 48% describe this statement as not applicable or not applicable at all. At the same time, 51% see (rather) no need to send messages to users of other OTT services.

---

[257] Cf. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, p. 23 f.

[258] Cf. e.g. *Arnold/Schneider*, An App for Every Step: A psychological perspective on interoperability of Mobile Messenger Apps, 28th European Regional Conference of the International Telecommunications Society, 2017.

[259] Cf. *Bundesnetzagentur (2020)*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, available at: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf;jsessionid=8426B6FF000026EC292A4CF57D316608?__blob=publicationFile&v=6, S. 23.

communication services. However, 43% would like to be able to do this.[260] According to the results of the consumer survey, there are two reasons for the almost equally high proportion of consumers who are not interested in interoperability. First, according to the survey results, multi-homing can be easily expanded. Overall, 26% of the OTT users surveyed said that they would in principle be willing to install another OTT service in order to be able to reach a specific user of another service. Secondly, it is still possible to fall back on the **classic telecommunications services** such as SMS or telephony if communication partners cannot be reached via messenger services. This is stated by 84% of the OTT users surveyed as completely or rather true.[261] In addition, 60% of respondents do not want to be contacted by users of other services. In the event that such contact would nevertheless be possible, 88% would

of the respondents want to decide for themselves whether to enable contact.[262] Retaining the power of decision seems to be very important for many consumers.

In a scientific publication in the journal "Telecommunications Policy", the authors come to the conclusion that an **interoperability obligation does not** correspond to **consumer interests.** Consumers would appreciate using selected messenger services for different contacts depending on the depth of the relationship. The psychological findings of the authors explained why consumers maintain a close relationship with certain messenger services regardless of network effects. The study is based on a survey of 2044 consumers in Germany who used messenger services such as Facebook Messenger, Line, Skype, WeChat and WhatsApp, but also e-mail and traditional means of communication.[263]

---

[260] Cf. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, p. 31.

[261] Cf. *Bundesnetzagentur* (2022) Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, p. 30 f.

[262] Cf. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung, p. 30 f.

[263] See *Arnold/Schneider/Lennartz*, Interoperability of interpersonal communications services - A consumer perspective, in: Telecommunications Policy,Vol. 44,Issue 3, April 2020, see *ScienceDirect,* available at: https://www.sciencedirect.com/science/article/abs/pii/S0308596120300197.

Insofar as an industry-wide interoperability project would be pursued, privacy compliant interoperability seems to be in line with consumers' wishes, which require such **active consent of users to be** reachable by other services. In particular, if a central directory service of users of the different services has to be created for the accessibility of other users, consumers seem to want to be asked for their consent before they are included in such a directory.

2. Desire for more data protection?

In surveys, consumers regularly express a strong need for privacy, but in practice they are comparatively careless with their private data. This contradiction is called the **Privacy Paradox.**[264] According to a study by the Sinus Institute, 93% of Germans consider the protection of their personal data important. Only 1% of respondents did not care at all about what happens to their personal data.[265] At the same time, a 2018 study by Bitkom found that WhatsApp is used by 81% of internet users in Germany, making it the most popular messenger service, while services that are considered by public opinion to be more privacy-friendly have a significantly

[264] Cf. for the following section and more detailed explanations *Bundeskartellamt*, Sector Inquiry Smart TVs, Report July 2020, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation /DE/SectorInvestigations/SectorInvestigation_SmartTVs_Report.pdf? blob=publicationFile&v=5 and the literature cited there, such as *Norberg/Horne/Horne*, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs 2007, 100 - 126, *Wiley Online Library*, available at https://onlinelibrary.wiley.com/doi/full/10.1111/j.1745- 6606.2006.00070.x. In the current academic discourse, however, there are a number of (behavioural) economic theories that can explain the privacy paradox. An overview can be found in *Barth/de Jong*, The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behaviour - A systematic literature review, Telematics and Informatics 2017, 1038 - 1058, see ScienceDirekt, available at: https://doi.org/10.1016/j.tele.2017.04.013. Finally, the privacy paradox can also be explained with the concept of so-called bounded rationality.

[265] *Sinus Institute/YouGov*, Study on data protection: majority of Germans doubt data security (2018), available at: https://www.sinus-institut.de/media-center/presse/mehrheit-der-deutschen- zweifelt-an-datensicherheit.

are less appreciated.[266] The underlying causes are complex and should not be allowed to obscure the limited **freedom of choice of** consumers ("reluctant"[267] - i.e. only with unwanted data disclosure or not at all[268]) and the lack of alternative offers due to a lack of competition. There could also be a **market failure** if no data protection-friendly offers are available on the market or if users cannot find out the data protection level of individual competing providers or at least not with reasonable effort.[269] These theoretical considerations seem to reflect the basic structures and mechanisms of action in the environment of certain messenger services. However, there are also **indications** that the aforementioned difficulties actually restrict consumers in their freedom of action: In an Allensbach study from 2019[270] , users of WhatsApp - i.e. people who have already decided to use the app despite any concerns they may have - stated that they did not agree with some clauses of WhatsApp's data protection provisions and would reject them if they were to use the app.

---

[266] *Bitkom*, Neun von zehn Internetnutzern verwenden Messenger (bitkom.org, 02.05.2018), available at: https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html.

[267] See *Borgesius/Kruikemeier/Boerman/Helberger*, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, EDPL 2017, 1, available at: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf.

[268] Cf. for this section *Bundeskartellamt*, Sector Inquiry Smart TVs, Report July 2020, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf?_blob=publicationFile&v=5 and the literature cited there.

[269] See *Botta/Wiedemann*, The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey, The Antitrust Bulletin 2019, pp. 428, 432 ff, available at https://journals.sagepub.com/doi/pdf/10.1177/0003603X19863590.

[270] Institut für Demoskopie Allensbach, Voluntary and Informed Consent? Die Nutzerperspektive - Untersuchung im Auftrag der *Focus Magazin Verlag GmbH*, September 2019; the results of the study were kindly made available to the Bundeskartellamt for the sector enquiry into smart TVs by *Focus Magazin Verlag GmbH.*

would have the possibility to do so. This includes, for example, the transfer of data abroad or access to the address data of one's own contacts.[271]

III. Investigation results

With the investigative questions, the Bundeskartellamt addressed the current situation and the opportunities and risks of interoperability in the run-up to the DMA from the perspective of the messenger and video services surveyed.

1. Interoperability in the area of tension between data security and investment readiness

The responses emphasise that there is no direct relationship between interoperability and data protection. Interoperability has no impact on how messenger and video services use personal data. A lower limit for the level of data protection in the market would be determined by applicable **data protection laws.** But when talking about interoperability goals, the requirements of data protection laws have to be taken into account. Interoperability complicates data security and thus also compliance with data protection regulations. In addition, interoperability reduces innovation, especially in the areas of data security and data protection.

The respondents did not refer to the MLS standard in this context.

The majority of respondents expect an interoperability obligation to have a **negative impact, especially on innovation, data security and data protection**. Interoperability would also run counter to consumer interests by impairing the user experience and preventing multi-homing, i.e. the maintenance of user accounts with several messenger services. A mandatory interoperability project would lead to the **lowest common denominator** in all the areas mentioned.

Some voices consider the problems associated with interoperability "not insurmountable in principle". Difficulties with data protection and data security could be solved on a technical level. One service refers to its own business model, the "heart" of which is interoperability. Reference is also made to the free messaging system Matrix. There, most of the challenges have already been overcome. For successful standardisation processes, there are also

[271] Institut für Demoskopie Allensbach, Voluntary and Informed Consent? Die Nutzerperspektive - Untersuchung im Auftrag der *Focus Magazin Verlag GmbH*, September 2019; the results of the survey were kindly made available to the Bundeskartellamt by *Focus Magazin Verlag GmbH* for the sector enquiry into smart TVs.

numerous examples. Ultimately, it is all a question of **willingness to invest,** all other Arguments, on the other hand, did not count, especially if companies with a "collar size" like Microsoft, Google and Facebook were involved. A globally active video service points out that messenger and video platforms were not developed with interoperability in mind. A technical redesign of the services would now require enormous effort and a significant willingness to invest. Some market participants explain that - viewed in isolation and detached from the negative interactions with innovation and consumer interests - **much is indeed technically possible,** especially with regard to data security.
Some video conferencing providers take a clear position here: an interoperability obligation would not bring **any additional revenue for video services.** Video services would already be accessible to each other in an adequate way. In addition to access via a link sent via the web browser, there are many freely available apps to establish connections to certain video services. Mutual access via interfaces is also possible. An obligation is unnecessary. The only result of mandatory interoperability would be less competition and poorer quality for users.
The extent to which quality competition can still take place beyond the possibly standardised functions in the case of interoperability was not discussed in the responses.

2. Voluntary existing or planned interoperability schemes

The Bundeskartellamt asked the industry whether and to what extent interoperability is already practised and whether further interoperability projects are to be implemented within the next 18 months. It became clear that the developments within the different provider groups are different.
When interpreting the results of the survey, it must be taken into account that the term **interoperability** can refer to **exchange arrangements with varying technical depth.**
Thus, individual **multi-messengers** describe themselves as interoperable. However, multi-messengers do not enable exchange across messenger systems. Rather, they offer a software interface that can be used to access different messenger services and read content. However, communication can only take place within one service. Otherwise, users have to transfer their messages to another service via "copy and paste".
With the **free messenger systems** XMPP and Matrix as well as the protocols or systems used for e-mail, there is interoperability among the respective clients of a system. The exchange in XMPP is based on the standardised XMPP protocol and is implemented via federated servers. For the

Access to certain other messenger and video services is offered through bridges[272] or bots[273] , but these cannot guarantee full interoperability. The Matrix client element emphasises that the bridges for Matrix are available to everyone everywhere, which is also mentioned by other interviewees. Bridges are available to Microsoft Teams, Slack, WhatsApp, Telegram, Signal, IRC, Discord and XMPP. An XMPP client states that there are interoperability solutions for enterprise use between XMPP and Cisco. A video service active in interoperability explains that there is a service unit operated by it through which third parties can connect to the enterprise. All technical specifications and more detailed provisions for the connections are up to the interested third parties themselves.

Finally, a distinction must be made as to whether messenger and video services offer all the prerequisites for establishing interoperability or whether this is actually already practised in bilateral or multilateral relations.

Many messenger and video services with an **open source philosophy** pursue interoperability as a business strategy or guiding principle. For example, providers such as BigBlueButton or Meet.jit.si, which call themselves open source, use open standards (e.g. WebRTC) that ensure interoperability and are fundamentally intended to enable interoperability with all messenger and video services.

Some industry participants offer third parties various ways to establish interoperability with them. In the case of "platforms" such as Rocket.Chat, for example, this is said to be done via **federation,** where - as with the free messaging systems - any server can become part of the network so that users of all connected servers can communicate with each other.

---

[272] A bridge can connect two computer networks. See for technical details *IP Insider*, What is a (network) bridge?, available at: https://www.ip-insider.de/was-ist-eine-netzwerk-bridge-a- 902076/.

[273] A bot (from *robot*) is a computer programme that performs repetitive tasks largely automatically without depending on interaction with a human user, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Bot.

In addition, a so-called WebHooks interface[274] is offered as well as **bridges and importers**[275] . With leading video services, consumers can first use reciprocal **access via a link in the web browser** without having to install the app of the other video service. According to some interviewees, this has been made possible by the **WebRTC** standard and is practised between many video services. Some video services also provide **public APIs**[276] (Application Programming Interface). Add-ins are also offered for a fee. In this way, users of Microsoft Teams could, for example, start a video call to Zoom from their user interface.

As far as bilateral arrangements or interoperability agreements aimed at specific providers are concerned, the services that focus especially on business customers are particularly active. According to the interviewees, this is due to the high demands on technical possibilities and the corresponding earning opportunities. In the course of these interoperability agreements, the video services Microsoft Teams, Webex and Zoom were mentioned in the survey. For business customers, interoperability is also initialised via **proprietary APIs.**

[274] WebHooks (composed of "web" and "hook") is a non-standardised method of server communication used in the context of distributed computing or message-oriented middleware. WebHooks make it possible to inform server software that a certain event has occurred and to trigger a reaction to the event, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/WebHooks.

[275] An importer is a software application that reads in a data file or meta-data information in one format and converts it into another format using special algorithms, cf. *Wikipedia*, available at: https://en.wikipedia.org/wiki/Importer_(computing).

[276] An API (Application Programming Interface) is a set of commands, functions, protocols and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so that codes do not have to be written from scratch. The API - also called the programming interface - thus enables applications to communicate with each other. The API is not the database or even the server, but the code that regulates the access points for the server and enables communication. This speeds up and simplifies the exchange of data between different systems many times over, see *Talend*, available at: https://www.talend.com/de/resources/was-ist-eine-api/.

Additional services in the area of interoperability are often chargeable. For business customers with special technical requirements, more effort is needed for video conferencing and the like. Business clients usually have special requirements, such as video rooms with cameras, microphones, touch screens or speakers. Very special software is used to operate this hardware, which makes access difficult. Technical

However, specialised service providers could produce this via selected "middle-layer software". Providers such as the Norwegian provider Pepix[277] are cited as an example. If interoperability is to be established via proprietary APIs, service providers such as Software as a Service (SaaS)[278] companies could also be used, such as the company Mio[279] , via which connections to leading video services such as Microsoft Teams, Webex, Zoom or Slack can be established. The open source project Matterbridge also offers bridges between a number of chat protocols. Supported protocols include XMPP, Slack, Discord, Telegram, Rocket.Chat and Matrix.[280]

3. Organisational and technical implementation of an interoperability obligation

a) Mandatory or voluntary?

The Bundeskartellamt also asked the messenger and video services how an interoperability project should be implemented. The choice was between a legal interoperability obligation, possibly also only for certain services, or a voluntary initiative. This was accompanied by a question about the participation of the own service and the reasons for the respective decision.

A **legal interoperability obligation** for all messenger and video services is considered helpful by only four respondents (all free messenger clients). It is argued that only a legal

---

[277] Cf. *Pexip*, available at: https://docs.pexip.com/admin/interoperability.htm.

[278] Software as a Service (SaaS) is a sub-area of cloud computing. The SaaS model is based on the principle that the software and the IT infrastructure are operated by an external IT service provider and used by the customer as a service. For the use of online services, an internet-capable computer as well as the internet connection to the external IT service provider is required. Access to the software is usually realised via a web browser. The service recipient pays a usage fee for the use and operation, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Software_as_a_Service.

[279] Cf. *Mio*, available at: https://m.io/external.

[280] Cf. Univention, available at: https://www.univention.de/produkte/univention-app-center/app-catalogue/matterbridge/.

commitment could restore user interests. Opening up to competitors would contradict the business objectives of the large services. Alternatively, an obligation of services from a certain number of users is conceivable.

A legal **obligation for the largest messenger and video services** can be imagined by less than a fifth of the respondents. Here, too, it is mainly a matter of free messengers and individual software providers. The most frequently mentioned services that should be made mandatory are the well-known messenger and video services Facebook Messenger, Signal, Telegram and also Threema, WhatsApp or Zoom (alphabetical order). Alternatively, according to the respondents, services with a user base that exceeds a certain threshold, such as more than one million users worldwide or the "TOP 10 providers" or services with a market capitalisation of more than 100 million US dollars could be subject to the obligation. One service interviewed states that the "operators of the leading operating systems" should be subject to an interoperability obligation. Another service also turns to the strong players in the market. They should at least refrain from taking technical precautions to prevent users from using or switching to competitors' software.

Just under half of the respondents can imagine an interoperability project based on **voluntary participation.** However, only less than half of those in favour would participate. These statements must be interpreted with caution, however, as both respondents who would participate and those who would not provided their assessment with numerous comments, preconditions, references and restrictions. This seems understandable, since the possible interoperability agreement was not specified in more detail by the Bundeskartellamt in its question, in order to avoid pre-determinations and corresponding controlled expressions of opinion.

Participation or non-participation thus appears to be a gradual phenomenon. The decision obviously depends significantly on one's own background as well as experiences and forecasts and certainly on the possibility of being able to **influence the development** oneself. In the end, all participants also point out that the evaluation of any interoperability regulations depends on many details. For example, the **technical depth or security that** is aimed at is decisive, e.g. whether it is end-to-end encrypted messages or rather an SMS format, which is much more insecure.

This assessment is also reflected in the fact that a large proportion of the reasons that tip the balance in favour or against are identical. **Negative effects on innovation, data protection and data security** are cited by a large proportion of respondents with both a rather approving and a sceptical attitude. Both groups also mention - although much less frequently - that an interoperability project is more difficult for smaller industry players.

than for large messenger and video services. This could make it more difficult for new market entrants to develop.

Overall, some messenger and video services that describe themselves as open source providers take a **relatively clear, supportive stance,** even without specifying the interoperability proposition. They fulfil the requirements for interoperability, which is also part of the business model and the conviction behind it. On the other hand, free messenger clients express themselves approvingly, which are more unknown to the general public: From their point of view, interoperability is important to break up the network effect and enable users to make decisions independently and voluntarily based on various criteria such as features and data protection.

Even well-known video services do not fundamentally reject interoperability. They already operate certain **interoperability agreements of varying technical depth and** offer the necessary interfaces. Especially in the case of the leading video services - according to the answers - the experience in global technical markets and the confidence to be able to set impulses here themselves and to influence the technical development play a role in their attitude.

Those messenger and video services that would not participate cite other, very different reasons in addition to problems with data protection, innovation and data security. One reason is often their **own business strategy, which does** not provide for interoperability. This is cited - e.g. by large foreign companies - for **cost reasons.** The development costs could not be refinanced. Clients who receive little attention from the general public express concerns about the enormous "**bureaucracy" and technical effort that** any interoperability project would cause, without explaining this in more detail. They also point to a **lack of market knowledge in** Germany, which does not allow them to make such far-reaching strategic decisions. Smaller providers focus on **niche offerings**, such as e-learning, or business customer groups that do not want interoperability and attach the greatest importance to **confidentiality and the highest security of** their data.

Two popular messenger and video services refer to the **legal requirements of** a possible legal interoperability obligation, as they were still required in 2021. Such an obligation may only be imposed if these are fulfilled. The remedy must have a positive impact on smaller competitors and encourage market entry. An obligation could only be imposed under the conditions set out in the second subparagraph of Article 61(2) ECAC, namely if "end-to-end connectivity between end-users (...) is threatened". This risk was not currently apparent. Traditional telephone services would be available everywhere. Multi-homing and switching providers would be possible for consumers at any time.

b) Functional and technical design

When asked which functions should be made interoperable, **text messaging** was named by slightly more than half of the respondents, **closely followed by group chats.** Telephony and video telephony follow close behind with about 40 per cent of the mentions.

When it comes to the question of how interoperability should be implemented technically, the implementation via **server interfaces is in** the lead, followed by bridges, a common protocol or by means of multi-messengers.

Not quite half of the respondents named **transport encryption** as the encryption method that should be used for interoperability, closely followed by end-to-end encryption. Several respondents emphasise that encryption should be user-selectable, as there are use cases for all combinations of transport encryption and end-to-end encryption.

As far as end-to-end encryption is concerned, many services have developed their own solutions. To trace these back to a specific standard would not be a trivial task. It can only be repeated, imposing a standard for a highly dynamic sector is complex, even if only a very basic form of interoperability is thought of. Some services agree, and can only imagine a narrow interoperability model limited to text messaging. Interoperability is "tricky". They themselves have gained experience over the last twenty years. There should be a core set of functions (for example, text messaging) that does not hinder **individual innovation.** These problems would have been solved years ago, but the "existing forces" would not have had a reason,

to take this into account. Therefore, legislation "with bite" would be important. A leading video service expresses similar views. The obligation should be limited to the **interoperable functions.**

Making certain specific functions interoperable would affect the innovation dynamic, as users would be less inclined to switch to different "platforms" and services would therefore have less incentive to develop new and innovative functions. Perfect interoperability would ossify existing technologies, which would become mandatory.

Two US services say text messaging and end-to-end encryption requirements would be less problematic than audio/video interoperability, although even interoperable text messaging would require some effort and cost. **Standardised server interfaces** would be useful for such an approach, allowing bilateral text messaging or group chat. **Standardised identifiers would** also be helpful for consistent messaging and prevention of misuse. One of the services considers multi-messengers to be the least disruptive measure.

Two services point out that the interoperability obligation does not **compromise quality** should mean. Interoperability can only be implemented on a small scale for Text - messaging via standardised telecommunication protocols with transport encryption. This would mean eliminating end-to-end encryption for user communications.

The choice of interoperability model, the type of technical implementation and the supported "Sub-functions" in detail should be implemented by the industry through open and transparent processes. In everything, **room for development** should be given. In the event that more detailed regulatory requirements were made, the interoperability of "cloud services" should be designed directly between the platforms of the services. An obligation should not pre-empt the MLS standard and thus put advanced end-to-end encryption at risk.

Furthermore, there are **different ways to achieve interoperability,** e.g. directly by everyone supporting a standard or indirectly via proprietary APIs through which the exchange can be established. An interoperability obligation should not freeze functions and innovations.

One service suggests separating the **operation of apps from the operation of messaging.** An obligation for "large central infrastructures" to grant access for "alternative clients" could be considered. In addition, it would make sense for apps from large providers to have a interface as well as enable a federative or at least inter-operational model for operating servers for message transmission. The existing e-mail servers and e-mail clients showed that this was basically possible. In addition, the "Matrix.org project" is another example that a definition and implementation of interfaces between the different components can be done in a perhaps more modern way than with the e-mail standards. However, it may be important to note that standardisation is not solely in the hands of the main players.

Some services did **not elaborate on the implementation of interoperability** because they reject it in principle. These services are leading services, services that advertise their high data protection standards as well as open source applications. The compulsion for interoperability is counterproductive. Another service states that it would then expose its own users to the risk that their data and usage behaviour would fall into the hands of other market participants with questionable business models. This is unacceptable for the service as it guarantees absolute confidentiality. A well-known video service also refers to the wishes of the users. A legal interoperability obligation is not in their interest. In the case of video services, mutual access already exists via the web browser. Anything beyond that would jeopardise the special functionalities of the app insofar as only the lowest common denominator would be possible. An open source provider also reiterates that interoperability could hinder the high speed of innovation in video conferencing.

be made. If there is to be an interoperability obligation, it must be kept as narrow as possible in order to hamper innovation as little as possible. The regulations should be **developed by the industry**.
In contrast, many free messenger clients have pointed out the **advantages of standardisation,** especially in connection with interoperability. The Federal Cartel Office asked the messenger and video services about the role of international standards. The comments on this can be read in the following chapter.

c) Interoperability through standardisation

The Bundeskartellamt asked the messenger and video services which existing standards for exchange and encryption could be used to establish interoperability. Half of the messenger and video services surveyed responded.
For **exchange,** WebRTC, Matrix and occasionally Acitity Pub[281] , RCS, SIP, RTP, SRTP as well as the standardised protocol XMPP, especially from free messenger clients, were mentioned. One service mentioned two standards in development, namely SFrame and Web Transport. For **encryption**, OMEMO was mentioned, the encryption standard from the XMPP world, as well as TLS and MLS, the Signal protocol, AES as well as DTLS, PGP[282] , RSA[283] , XMPP, WebRTC and Matrix.
Several free messenger clients state that the **use of uniform standards** is indispensable for interoperability. With XMPP, a standard for message exchange in the broadest sense was already created in 1999 and has since been further developed by the XSF (XMPP Standards Foundation) and the IETF. The IETF had also developed other widely used standards for e-mail or websites (HTTP) or would continue to develop such standards.

---

[281] ActivityPub is an open, decentralised social networking protocol released in 2018 and managed by the W3C. It provides a client-to-server API for creating, uploading and deleting content, and a server-to-server API for decentralised communication, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/ActivityPub.

[282] PGP is used to encrypt e-mails and is the basis of OpenPGP, a widely used e-mail encryption standard, cf. https://www.openpgp.org/.

[283] RSA (Rivest-Shamir-Adleman) is an asymmetric cryptographic method that can be used for both encryption and digital signing. It uses a key pair consisting of a private key, which is used to decrypt or sign data, and a public key, which is used to encrypt or verify signatures. The private key is kept secret and cannot be calculated from the public key with realistic effort, see chapter D.I.4.a or see *Wikipedia*, available at: https://de.wikipedia.org/wiki/RSA-Kryptosystem.

Moreover, at least Facebook Messenger as well as WhatsApp, Google Talk and KIK Messenger would even have been based on XMPP. This means that the companies involved would have used the standardised and public protocol XMPP (and ejabberd as one of the freely available open source server implementations of XMPP) to create their product on its basis through **proprietary (in-house) extensions that they did not feed back into the public standardisation process.** It would have been easy for these companies to bring their changes and extensions into the standardisation process from the beginning, so that everyone would have benefited. In contrast to adhering to international standards, these companies benefit far more from incompatible stand-alone solutions because users are forced to open an account with the large service providers, which allows these services to gather a lot of users and to collect and analyse their data. Such a position of power also invites the misuse of data, as users cannot easily switch to other alternatives due to the monopoly position that has been created.

With e-mail, on the other hand, a messaging system had been created that allowed users maximum freedom with regard to the choice of provider (they could even operate their own e-mail server and thus be independent of third-party providers). A similar system for real-time communication via "chat" and (video) telephony was more than desirable - indeed, it even made economic sense and was socially necessary.

The **mandatory cooperation of different provider systems** (targeted interoperability) is a possible solution to bring the large providers of free chat services to interoperability. For the providers of commercial chat services, the goal is achievable through public and private tenders, in which **compliance with a standard protocol** (XMPP) must be an essential element. In this way, providers could independently adapt their systems accordingly if they want to reach commercial users.

In the opinion of the services interviewed, only those solutions should be used in politics, administration, authorities and offices that meet this requirement or are likely to do so.

4. Impact of interoperability

Finally, the Bundeskartellamt also questioned the industry in detail about the general effects of interoperability. The results of the investigation are first presented in an overview (see a)). Subsequently, comments on individual aspects are presented in more detail (see b) to g)).

a) Investigation results at a glance

Specifically, services were asked how the establishment of interoperability would affect their service in terms of user numbers, revenues, intensity of competition, level of data protection, level of data security and innovation. Respondents could choose answers between "very negative" (-2) and "very positive" (+2).

In order to be able to present the different answers in a meaningful way, the services surveyed were assigned to five different groups as far as possible and a separate evaluation was made for each of these groups.

- Large closed messenger systems (6 services)
- Leading video conferencing services (4 services)
- Competing video services (9 services)
- Free Messenger Clients (12 services)
- Open source services (5 services)

A total of 7 interviewed services could not be **clearly assigned to any of these groups** and could not form a separate group due to their heterogeneity. However, particularly relevant assessments or explanations of these services are presented selectively in the following evaluation.

When asked about the impact of interoperability on their own service, the following average assessments emerged for the different groups (see Figure 14):[284]

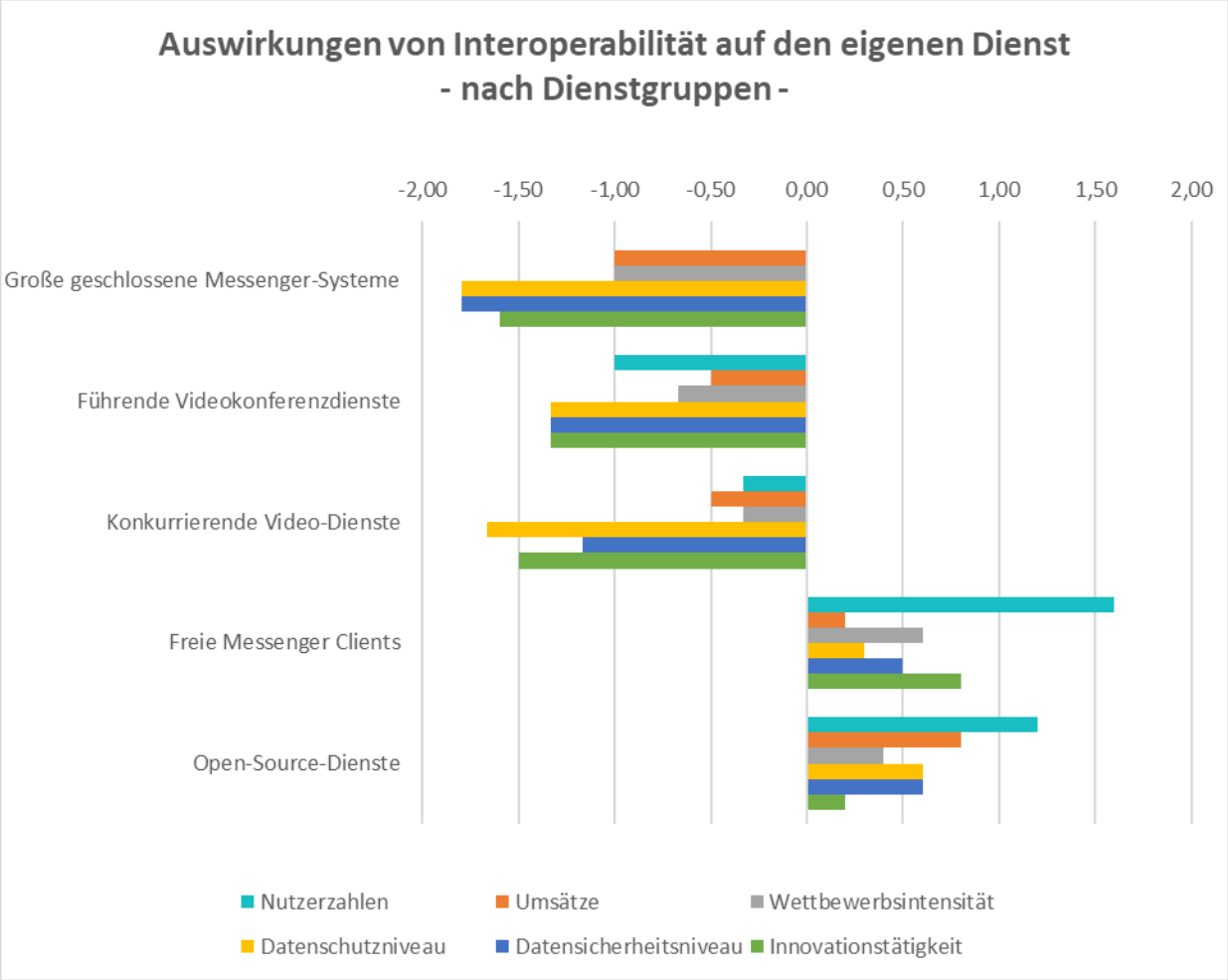


Figure 14: Impact of interoperability on own service - by service groups

If the identification results are not aligned according to the different groups of services but according to the different impacts of interoperability, the following picture emerges (see Figure 15):

[284] When evaluating the results of the survey presented below, it must be taken into account that the number of services belonging to the individual groups varies and that the market importance of the individual services (and groups) is very different. Furthermore, only average values for each group are shown; the assessment of individual group members may well deviate from this. The average value "O" is not visible in the graph.

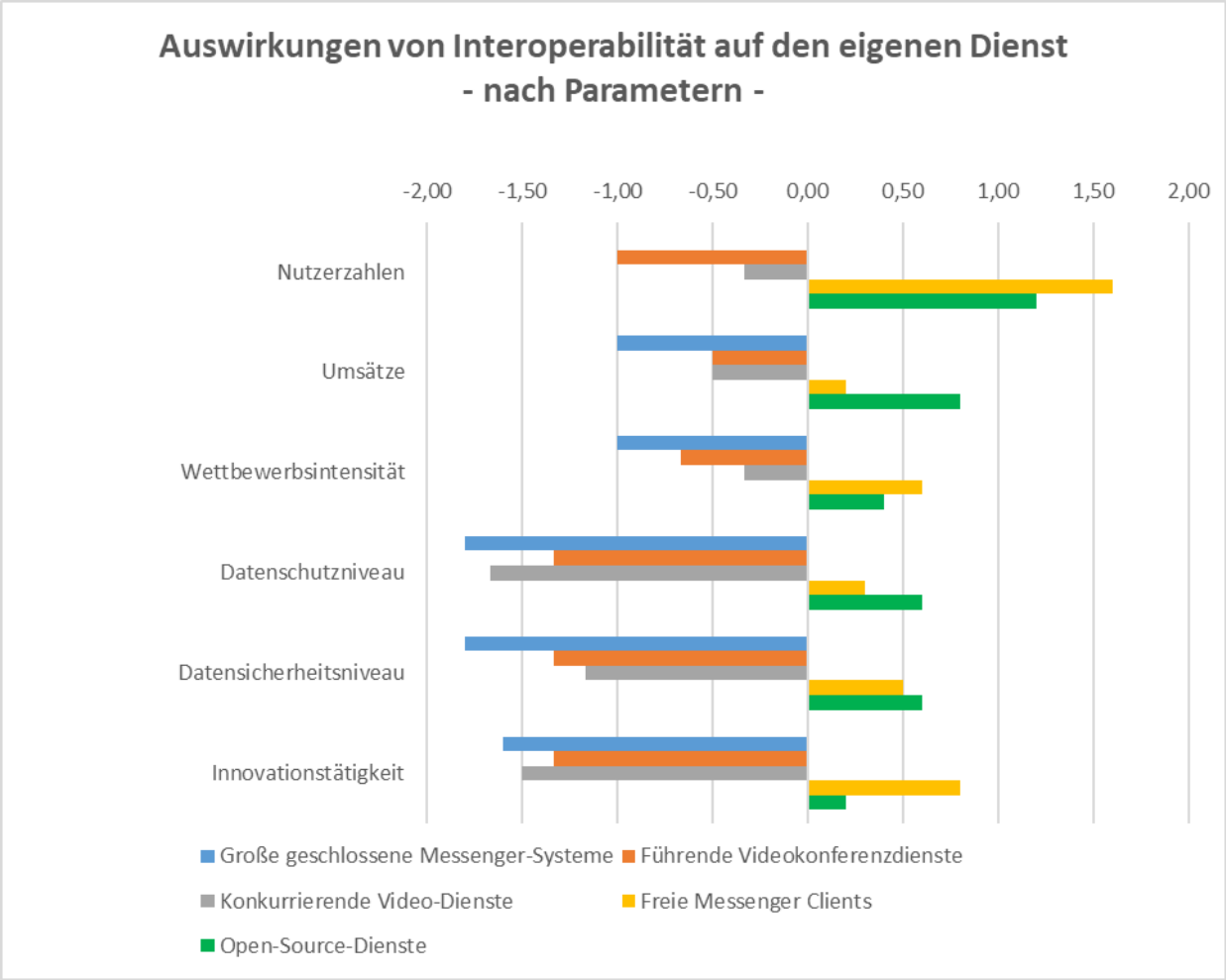


Figure 15: Impact of interoperability on own service - by parameter

The two graphs clearly show that both the large closed messenger systems and the video conferencing services expect negative effects of interoperability for their own company overall. The large closed messenger systems were particularly negative. Only with regard to their own user numbers do these services expect no effects on average (the bar is not visible with the value "0"). The strongest negative effects are expected by the three groups mentioned for the **level of data protection, the level of data security and the innovation activity of** their own service. Services that advertise with particularly intensive data protection measures also expressed criticism in this context. These are not included in the groups defined above.

The groups of free messenger clients and (small) open source services, on the other hand, expect positive effects of interoperability on their own service. The development of their own user numbers is seen as particularly favourable. The open source services also expect positive revenue development.

Some services also gave more detailed reasons for their assessments. However, some services also emphasise the high dynamics of the market in this context, which makes it almost impossible to predict developments:

Several free messenger clients expect higher **user numbers** for their own service, as it would receive greater attention and be more accessible if it were interoperable.

"Binding to island systems" would no longer apply. Overall, according to this assessment, users would - as with email - be more strongly distributed among different services. At the same time, however, a free messenger client points out that the number of installed apps/clients for the industry as a whole would decrease, as users would no longer have to install several service apps at the same time with interoperability. Two other services, on the other hand, suspect that users would be more likely to **switch to the market leaders for** reasons of convenience, as the differentiating features of the smaller services would disappear through interoperability. One leading video service fears that the agreement on the lowest common denominator associated with extended interoperability could reduce the attractiveness and thus the demand for video conferencing services overall.

In terms of **revenue,** several services point to the positive correlation between user numbers and revenue, at least in the business sector. Two leading services that are popular with consumers expect a decline in revenue from business applications, as quality and user experience would deteriorate due to interoperability. Another (paid) service, which advertises a high level of data protection, points out that private users would no longer be willing to pay if the (supposedly) same product were offered free of charge by another service.

The services surveyed also gave quite different assessments and reasons for the effects of interoperability on the **intensity of competition** and **innovation.** Both proprietary and open source videoconferencing services state that competition between services is currently already intense and would tend to be reduced by interoperability if it limits innovation and differentiation opportunities. Several services from all groups also tend to assume that innovation activity - as with telecommunications or e-mail - would slow down and interoperability could at best lead to a strengthening of the large ("American") providers or competition between them. Several free messenger clients or open source services, on the other hand, expect competition to intensify (in their favour) and, consequently, innovation to increase, since users could switch more easily with interoperability. The reasons given for this central assessment question clearly show that the interviewees have different ideas about this.

whether or not (sufficient) **differentiation possibilities for** the individual services are retained in the case of interoperability and how the users react to this.

With regard to the **level of data protection** and **data security**, individual services point out that "large services with poor data protection standards" would then also have access to the data of other services. According to this assessment, a common identity management and the multitude of new interfaces would have a negative impact on data security. In addition, critics of interoperability again fear standardisation at the lowest common denominator. In contrast, some advocates argue that users could then switch to services with a particularly high level of protection or security. The standardisation of interfaces and the decentralisation of data processing would already lead to an improvement of the current level. Finally, some services emphasise that data protection is regulated by law and interoperability is unlikely to have much influence on this. The services' explanations of this statement also show that the market participants have very different ideas about the effects of interoperability on **data security and data protection.** This is probably due to the different business models and diverging assessments of consumer behaviour.

In another question, the messenger and video services were asked to indicate the extent to which they agree with certain **statements on the topic of data protection and interoperability** (see Figure 16). The theses were: "The level of data protection in messenger and video services must be improved", "The level of encryption in messenger and video services must be improved", "Interoperability of messenger and video services is desirable in principle", "The establishment of interoperability should be prescribed by law", "A legal requirement for interoperability in messenger and video services is desirable in principle", "The establishment of interoperability should be prescribed by law". mandatory interoperability would mainly benefit the big messenger and video services", "Consumers in Germany would like to see interoperability of messenger and video services". The scale of answer options here again ranged from

"Do not agree at all" (-2) to "Fully agree" (+2).

Unlike free messenger services, open source services and competitors of the leading video services, the major messenger services and the leading video services see no need to **improve the level of data protection**.

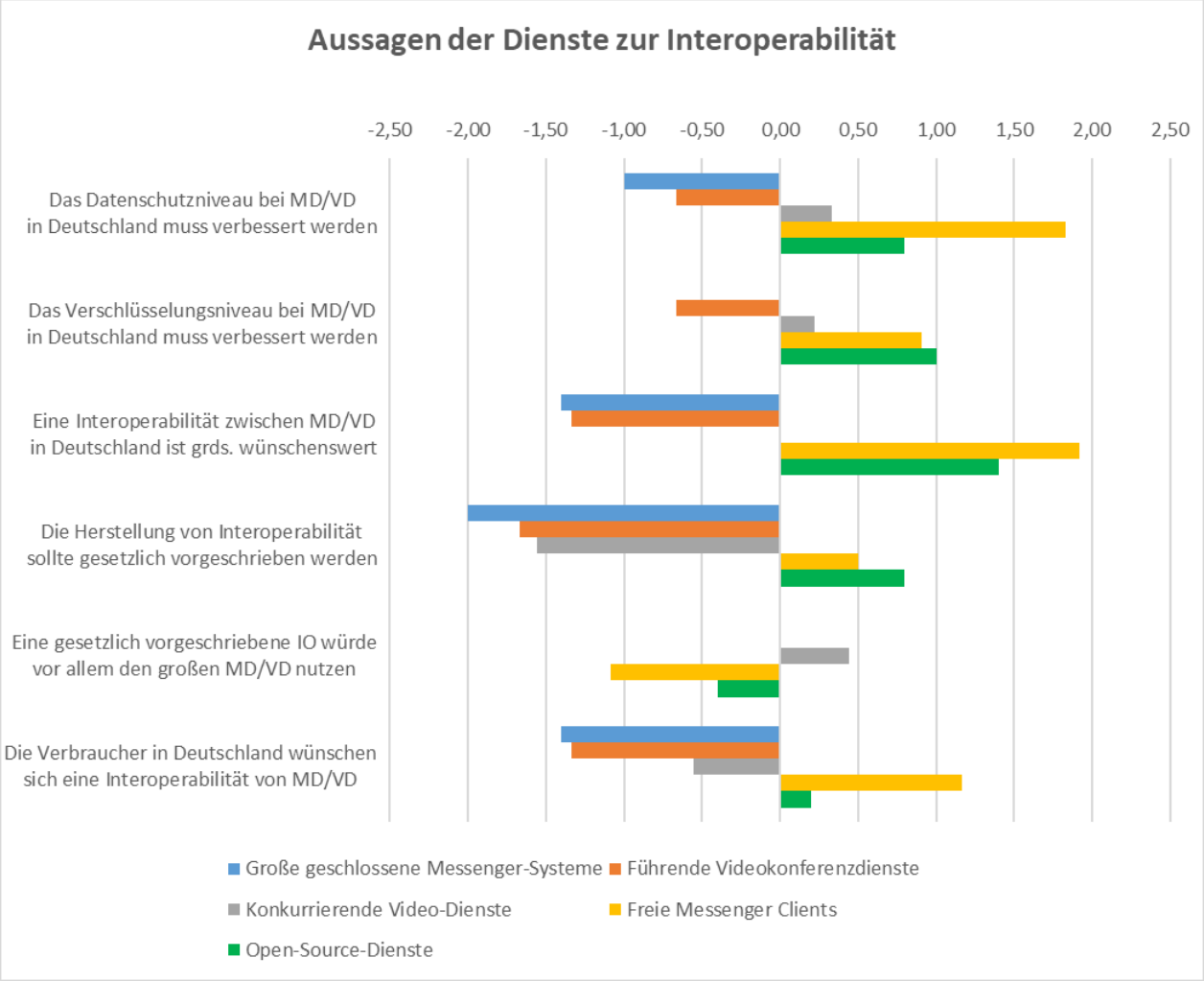


Figure 16: Statements on interoperability

As far as the **level of data encryption** is concerned, on average there is no clear opinion of the large closed messenger systems (no bar at value "0"), while the leading video conferencing services have reacted negatively.

The statement that **legally mandated interoperability** would primarily benefit the large services is assessed inconsistently by the stakeholders (no bar): Two major services fully agree with this statement and two other major services disagree with this question. The answers of the competing video services are somewhat more differentiated compared to the major services: on average, they see a slight need for improvement and advantages for the major services, but rather no consumer desire.

The assessments of the above theses also show that the large closed messenger systems and the leading video conferencing services clearly reject the possibility of **legally prescribed interoperability.** In contrast, the answers of the free messenger clients and the open source services are clearly in favour of interoperability.

A corresponding legal provision is supported here. Overall, these services tend not to see the danger that legally prescribed interoperability would primarily benefit the large messenger and video services; however, two of these services fully agree with this statement, as do two particularly data protection-oriented services that are not included in the aforementioned groups and the graphical representation. In the (optional) justifications for the assessments given, various aspects are addressed by individual services, which are presented in detail in the following chapters and will only be briefly summarised here: Several respondents state that the use of a common **international standard** such as XMPP is crucial and that this should be taken into account in public tenders, for example. Some services point out that it would be easier for large messenger and video services to cope with the **technology burden** required to achieve interoperability, while this would be a significant burden for small services. Two large services popular with consumers stress that only the rules of the European Electronic Communications Code (ECEC) would govern a possible interoperability obligation and that these should not be undermined by divergent national rules. An inclusion of an interoperability obligation for messenger services in the catalogue of obligations of the DMA was not yet foreseeable at that time.
Regarding the **wishes of consumers,** some services state that they would complain about the large number of different apps; other services emphasise that the parallel use of different apps is fine for consumers.
Individual services also point out that consumers do not really know what interoperability could actually mean.
However, the issues that most concern services are the possible impact of interoperability on the offer of innovative functions and the possibility to differentiate themselves even under interoperability.

b) Innovation incentives and differentiation opportunities

The vast majority of respondents say that interoperability and the associated standardisation would **inhibit innovation processes and weaken product differentiation.** The lowest common denominator would have to be agreed upon, which would also lead to misallocations. Both services with a focus on messaging, which are particularly popular with consumers, and well-known video services argue uniformly on this issue. Since interoperability would make the offerings more uniform, customers would be less inclined to switch between services. In turn, services would have less incentive to offer new services.

develop innovative functions. "Perfect interoperability" would "concretise" technologies that would be the standard of engagement.

A leading videoconferencing provider points to already existing lively competition in the consumer and especially in the business customer segment. There are a number of services competing intensively for customers, especially business customers, both on price and on the development of new features. Competitors explain that video services are differentiated from each other by the different functions they offer in **addition to the core functions of** audio and video transmission. This applies not only to the business customer segment, but also to consumer offerings. This included, for example, hand raising, emojis in conference chat, sharing content, playing visual backgrounds, etc. If screen sharing or presentation modes no longer worked during video conferences because some of the services involved through their users did not support them, further developments in this area would not make sense. In this way, only the lowest common denominator would be reached. The industry can only move forward as the slowest participant can keep up.

This is even more true for more complex functions, even in the **business sector**. Certain video functions could be integrated into data processing or spreadsheet programmes or presentations. If this is no longer possible for all users under mandatory interoperability, this goes against their interests. Providers would then no longer invest in such functions.

Some providers cite **examples** of areas where interoperability has stalled innovation in the past. One open source service draws a comparison with traditional telephone services. These would be interoperable, but there are tight limits to what each service can implement. If other services do not support "HD Audio", for example, one's own offer cannot be realised. This **innovation gap in traditional telephony** has given rise to messenger services, which can bring new functions and capabilities to the market relatively quickly. This would probably be lost if the services were standardised and any new functions had to work with the agreed standards. As a negative example, reference is also made to the **development of e-mail**, which has technically come to a standstill at a certain point. From a data protection point of view, there would also have been no further development at some point.

Individual competitors of the leading services complain that **complexity** also increases when interoperability has to be implemented. Customer service and support for users would become more difficult and require more time and effort. Teams of developers would have to be dedicated to this instead of developing new and innovative features. This process challenges and disadvantages smaller competitors in particular. If interoperability is forced and

functions would be standardised, this will **favour the big companies**. They would set the standards according to their purposes/needs and resources. Smaller competitors would have to adapt their products to them, at the expense of the innovations they would otherwise have developed. This would have two effects: First, innovation and product diversity would decrease at the expense of consumers. Secondly, the **supremacy of the largest players would be** cemented. The migration of small competitors would be foreseeable, as they would be deprived of their possibilities for differentiation.
Possible future open source implementations of a standard, e.g. Open MLS, are not addressed in the responses.
The "consumer internet" had been so successful so far because "innovation without permission" was possible. Compositions (so-called "sets") of functions were not standardised, so that smaller, innovative companies were able to develop business fields alongside the large competitors.
It is again some free messenger clients and individual other voices that argue otherwise: With interoperability, many independent services with **new ideas** would have **a chance**. The large commercial providers of chat services would face stronger competition because users could switch more easily. Through increased competition and compliance with a common interoperable standard, the providers of clients or even server services would have to distinguish themselves from other services through **other unique selling points**, such as a particularly easy-to-use user interface. This increases innovation. The established providers could no longer rest on their large user base. Companies could focus more on feature development and it would be easier for new players to enter the market.

c) Consumer interests (user experience and multi-homing)

aa) User experience

Several services take the perspective of consumers and are concerned about the user experience. Different assessments also result from the fact that the services are positioned differently. For example, there are social media platforms focused on a multi-functional user experience compared to services focused on secure or privacy-friendly messaging or advanced video conferencing.
Various operators of social media platforms state that even if all possible time and resources were invested in an interoperable messenger service, the functions would not be comparable with the current offer and would no longer be interesting for users. The **user experience** would then be inferior. This would also apply if interoperability only led to a

agreement on basic functions, and further **additional functions** could be operated alongside them. Apart from the fact that this would also be extraordinarily costly, the demands of today's users could not be met. The **offer of additional functions such as surveys, stickers, shops, catalogues, payment forms in chat apps also runs via servers, which could** probably not be maintained with interoperability. Another service also explains that **servers are configured in such a way that there** are **certain channels for certain topics.** This could not be made compatible with other services. Interoperability only for the messaging function would theoretically be conceivable. But then the user experience, especially for voice and video messages, would be greatly reduced. One would have to orient oneself to the service with the worst performance.

The interoperable product is likely to be similar to SMS, a product that does not have video or audio elements, is not encrypted or can only be provided with limited security measures. Such an outdated product could not be offered. It would also not be desired by consumers. They would expect a different user experience from their service. Successful products emerge from dynamic competition with constant further developments and improvements. This does not happen under interoperability.

In general, interoperability would also make it more difficult to implement platform "standards and policy" and to address abuse.

Another interviewee also points out that for consumers, it is
might be difficult to understand if they have certain functions, such as "polls" or "self-destructive messages" under interoperability no longer or then only with female users and users of the same service.

bb) Multi - Homing

Finally, several messenger and video services primarily used by consumers indicate that consumers use different communication channels for different needs (multi - homing). For example, WhatsApp would be used to communicate with family and other services for professional purposes. Mandatory interoperability would take away this flexibility from consumers.

There is no evidence that consumers need interoperability "unless you feed them misleading statements, e.g. that video telephony should work like voice telephony".

Multi - homing would be widespread and appreciated by consumers. Most services could be used from different devices at no additional cost. Users could tailor their messenger world and use certain functions for certain tasks or user groups (e.g. one service for family, friends, one for business, etc.). Depriving consumers of this possibility is not in line with the principles of competition policy.

d) Data security

According to the majority of the industry, the decreasing incentives for innovation under interoperability would also affect developments for data security. The industry participants responding in this way predict that a lower limit - the lowest common denominator - will be created in the course of interoperability. In particular, services known to be data protection-friendly put forward this argument.

Some respondents also mention fundamental security issues, such as that opening up one's ecosystem to other services limits the ability to prevent spam and fraud. Another service says that interoperability opens up secure systems to services that do not take data security seriously. Most market participants, however, focus on encryption (see aa)) and identity management (see bb)).

aa) Encryption

A globally active service refers here to the development of the **MLS standard**. In any effort to achieve interoperability, data security must be kept in mind. An interoperability obligation should not pre-empt adoption. This would then be at the expense of data security in the form of advanced end-to-end encryption.

Many other messenger and video services question whether secure encryption can be implemented under interoperability. Since end-to-end encryption does not work under interoperability, according to their account, many external APIs would have to be provided that could be abused.

The messenger and video services, which see only the lowest common denominator in the course of interoperability in questions of encryption, name transport encryption as such. It is not possible to maintain end-to-end encryption under interoperability. For this, all providers of interoperable functions would have to use the same protocol. Other respondents state that **end-to-end encryption** must be developed across providers and protocols under interoperability. Technically, it is a matter of agreeing on a standard that enables end-to-end encryption under interoperability.

The difficulties would lie in **video communication and a multi-point end-to-end**

encryption with the exchange of keys between different providers. In addition, users' devices must be capable of running the sophisticated software. Older or less good devices would be at a disadvantage, which could exclude users from the services. A multitude of service providers would probably be necessary to manage the **server infrastructure, which would** make everything even more complicated. Standardisation would require all parties to agree on how the technical infrastructure would be designed, who would be responsible for hosting and server management. All this would require significant investment and probably take years.

Some free messenger clients are more positive about the impact of interoperability. The standardisation of interoperable interfaces will increase the level of data security.

Consumers could switch to secure messenger and video services.

bb) Uniform identifiers / identity management

If end-to-end encryption is to be implemented, **identity management that** can work with the many different services is required, according to some respondents. Messenger and video services use different **identifiers**, i.e.

Identifiers by which users can be uniquely identified and registered. This can be - as described in section D.II.1. - e.g. a mobile phone number, an email address, an ID or a chat account, which must then be entered or created in order to use the service.[285]

Leading messenger and video services such as Facebook Messenger, Discord, iMessage/FaceTime, Microsoft Teams etc. use their own identifiers. Corresponding management is a technical challenge that also places high demands on data protection. There must be **mutual access to all identity information** between all interoperable messaging and video systems. At the same time, the security of **meta-data** must be guaranteed. A technical solution for this does not yet exist.

One service, which is aimed in particular at users who attach great importance to data protection, sums up that all this is certainly not in the interests of consumers. For users, the **security of communication** becomes **intransparent and uncertain**. The provider also states that users do not know which app the other person is using.

---

[285] Cf. *Kuketz*, Die verrückte Welt der Messenger - Teil 1, p. 7, available at: https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/.

e) Data protection

Positive effects of interoperability on data protection are expected by some free messenger clients and individual other voices, while the majority of respondents express concerns.

Users would be able to **switch** more easily to privacy-friendly and secure services under interoperability. Services that would offer worse data protection compared to a common standard then applicable under interoperability would have a competitive disadvantage that they would have to eliminate.

The respondents who express concerns speak - as with data security - of the lowest common denominator, which is only practised under interoperability in data protection (example: using the telephone number as an identifier). Even today, the large platforms would not be under control in terms of data protection law.

The main challenge would then be to motivate services to achieve more than the **lower limit** in terms of data protection. Instead of different levels of data protection offered by services (with the lower limit of the GDPR), as is currently the case, the market under an interoperability obligation would only reward if the lower limit is reached, nothing more.

Innovations for data protection or data security would be lost.

In addition, **personal data** would be distributed **among several providers,** whose reliability might be in doubt. One video service shares this concern and explains it as follows: Until now, it has been possible to protect against "data loss", for example, by not being able to "cut and copy" business information from business messages.

and to carry it to the outside world. But if this could no longer be monitored by the service alone under interoperability, this protection would be lost.

Further data protection problems are triggered by the **international nature of** the underlying business, according to industry sources. One German provider doubts that European and American data protection authorities will agree. Another European service points to a **lack of data protection with non-European providers**. Some services are concerned that if interoperability is achieved, personal data will be accessible to untrusted services from abroad. Legal enforcement and auditing are also important for details.

Even during the standardisation process, consumer rights would have to be enforced and consumer rights violations would have to be prosecuted if large market players did not comply with the rules.

Against international data collectors, only "full encryption" would help, with availability of the source codes at least of the client software, to prevent the app from being copied and used elsewhere.
Centralisation in interoperability is also mentioned by some respondents as a risk to data protection, especially when it comes to **meta-data.** Communication meta-data would be highly explosive for data protection. The more different services are integrated into communication, the more points of attack there are for spying on this data. Centralisation is a dangerous dynamic for this, as suddenly all this data is in just one place, which increases the attack surface just as much. This dilemma can only be solved in a serverless, distributed communication network. Another sensible way of dealing with this is to offer different tools and leave the solution of their problems to the users themselves.
This raises the question of **who monitors** or has access to the **centralised data** and how consumers can still exercise their data protection rights. The services themselves would have to share their data with other messenger and video services and would lose control over their users' data, but would still be responsible for offering all functions.

f) User numbers and turnover

Several leading services from both the consumer and business segments expect their offerings to become less attractive and user numbers to decline as interoperability forces them to agree on the lowest common denominator. As a result, the "user experience" suffers in the wake of poorer service quality, which has a particularly negative impact on business customers.
- customers will have a negative impact. Some competitors of the leading providers also expect a **decline in user numbers** for their services in the course of interoperability. If differentiation opportunities disappear, **network effects would again** become **more important** and the market leaders would become more attractive again.
The answers did not address whether and to what extent individual functions can be offered by the messenger and video services in addition to the standardised interoperable functions in the case of interoperability.
Smaller video services have other expectations: Interoperability would **lower** the **barriers to** using video services. **More niche services** would become available that better meet the needs of consumers.
An open source provider does not expect any special effects. The corresponding offer is already widespread.

Many free messenger clients expect user numbers for their applications to increase if there were market-wide interoperability. Users would distribute themselves among the services if there were no more closed systems. More users could be reached, so that not so many messengers would have to be operated at the same time. Better exchange possibilities would make users aware of existing solutions. Interoperability with the large services that were previously closed off would also increase the **attractiveness of the open network**.

Overall, the industry does not seem to expect any significant changes for the development of **turnover** through interoperability. In some cases, negative expectations prevail. For services that expect decreasing demand due to poorer quality of an interoperable feature set as well as services that fear customer churn, the situation will be reflected in revenues. One privacy-oriented service sums up with "nobody pays when it's the
ostensibly the same thing for free".

g) Competitive intensity

The assessment of the intensity of competition shows a very mixed picture.

Some video services describe their competitive environment as highly competitive. Established household names compete with new entrants and niche players. One service says it also differentiates itself from its competitors by offering a wide range of interoperability solutions.

A free messenger client also fears the **loss of its unique selling point**, namely interoperability. Due to the reduced possibilities for differentiation, a decreasing intensity of competition under interoperability is also expected from other video services. Investments in product quality and security would no longer pay off.

This argument is also used in the more consumer-oriented messaging sector: If small services could no longer distinguish themselves through special offers in the course of an interoperability obligation, users would migrate to the large platforms. The position of the **market leaders would be cemented** and competition would weaken. One service suspects that competition will then mainly take place between the large American platforms.

Individual voices consider exactly the opposite reaction likely: interoperability would lead to smaller companies with **niche offerings** becoming more attractive to users of larger services. In contrast, some other free messenger clients also expect **increased competition** if consumers were no longer bound to the island systems in the course of mandatory interoperability and could switch more easily.

5. Interoperability and standardisation in the light of industry interests

a) The right way?

The imposition of a possible complete standardisation process in the course of a particularly mandatory interoperability project is viewed critically by the majority of messenger and video services. It is discussed to what extent interoperability is suitable for the markets concerned to achieve positive effects. Normally, competitive and dynamic markets are associated with interoperability.
Interoperability is an appropriate means for standardised, homogeneous services with high market penetration such as telephony or retail banking. However, from the point of view of the industry companies, an interoperability obligation would also be associated with great risks. In the markets in question here, innovations would be prevented in all essential questions.
"Without innovations, probably only the Facebook group would remain in the market, alongside which only a few others could continue to exist. There would also be a massive administrative and technological burden".
An internationally active interviewee emphasises again that there are basically **several ways in which interoperability** can be achieved. Standardisation is only one of them. Their own company offers a variety of interoperability solutions. This is done in such a way that innovation does not suffer. The solutions offered also include a platform based on known standards, which allows third parties to communicate not only with their own company, but also with certain third parties. Interoperability is also possible via proprietary APIs that others can use to connect (e.g. via service providers).
Many leading services in the industry emphasise that they want to support interoperability projects on a voluntary basis, provided that the **quality and safety of the products are** promoted. Some emphasise that this is already happening through participation in the **development of the MLS standard. The** adage "the perfect (interoperability) is the enemy of the good (user)" also applies to interoperability. experience)".
In general, obstacles would already lie at the **political level**, namely in the question of whether large services would participate. In any case, the implementation of an interoperable standard would not necessarily result in an interoperable system.

b) Challenges and risks

One respondent describes in detail that interoperability is a challenge. It is actually prohibitively expensive and can only result in a standardisation process. However, it is competition that brings about improvements in data protection and data security for consumers, not standardisation. Incentives to innovate would be absent if there was a standard that would

also produces a fixed level of data protection and security that is not further improved.
A comprehensive standard for all market participants could not do justice to the **technical complexity** and dynamics of the market. Since the various protocols and data formats differ greatly, it would probably be very difficult and costly to enforce a standardisation of protocols and data formats.
Large and small market players argue that especially **smaller market participants** would be disadvantaged in such a process. If their own offers and functions had to be adapted according to the specifications, this would tie up developer resources for a longer period of time, which smaller companies could not cope with. They would be set back in the competition.
Another service points out that minor incompatibilities could lead to fragmentation, as is the case with XMPP, for example. Some video services argue similarly and illustrate problems of standardisation using the WebRTC standard: many existing messenger/video services would not be compatible with the WebRTC 1.0 standard. Different protocols for "signalling" make interoperability complicated, even though the WebRTC standard is
is used. Even if all platforms used a standard for video etc. like WebRTC, there would still be differences in the network layer and "signalling" depending on the network infrastructure. If every service was forced to be interoperable, they would all have to leave their own secure network. This in turn would hamper innovation within security development.

c) Implementation

Individual respondents problematise in detail a possible implementation of a standardisation project.
If authorities wanted to make demands on the industry in terms of interoperability, the requirements, the selection and the definition of the desired interoperable functions would have to be specified at a **high technical level.** The decisive factor is what is regarded as the benchmark in a rapidly developing environment. Standardisation as well as faulty adaptations or adaptations not in line with the market could be the result of wrong decisions.
It also depends on who makes the specifications. It has to be the **industry** that identifies the goals as well as the global standards and continues to develop them in order to meet the requirements. This is the only way to prevent obsolete technologies from being codified.
In any efforts to achieve interoperability, **the requirements of data protection laws and data security** must be kept in mind. Currently, the MLS standard is under development. A

interoperability obligation should not be allowed to pre-empt adoption. This would then be at the expense of data security in the form of advanced end-to-end encryption.

Finally, interoperability should only be implemented on the basis of **global technical standards.** In a global world, interoperability requirements should not be formulated on the basis of national or regional standards. It would be very burdensome for the industry to have to meet different requirements worldwide and to offer different sets of interoperable functions. At a certain point, this would no longer be sustainable. Global technical standards create global markets. If national or regional authorities imposed interoperability obligations, smaller markets would emerge within the global action space. Accordingly, more programming would have to be done. The longer the programme codes become, the more errors can creep in. This leads to higher costs and more time for corrections.

d) Suitability of market participants, institutions and authorities to contribute to a standardisation process

The Bundeskartellamt asked the messenger and video services who they considered suitable to contribute to a standardisation process. The answer had to be justified in each case.

A good 60 per cent of those surveyed said that the **IETF (Internet Engineering Task Force) was the** most suitable body for implementation through standardisation. In a global world, local solo efforts would not prevail. This opinion is present in all groups, i.e. it is held by open source solutions, free clients as well as leading providers. In the opinion of the respondents, the IETF has above all the necessary experience for this task. The IETF has already developed numerous interoperable standards, especially protocol standardisation, for the Internet and promoted their implementation. XMPP, TLS[286] , SIP[287] and WebRTC are mentioned as examples. The IETF also has the necessary independence. It is an independent task force that works towards an overriding goal and does not primarily evaluate national interests. One interviewee agrees in principle, but notes that its success so far has been based mainly on

[286] Transport Layer Security, also known under its predecessor name Secure Sockets Layer, is an encryption protocol for secure data transmission on the Internet, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Transport_Layer_Security.

[287] The Session Initiation Protocol (SIP) is a network protocol for establishing, controlling and terminating a communication session between two or more participants, cf. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Session_Initiation_Protocol.

Areas such as "infrastructure/transport/access layer" with standardised services and less on Use cases in the highly differentiated area of "service layer".

Just over 25% of messenger and video services believe that the **EU Commission** should also be involved in a standardisation process.[288] A leading messenger service states that the European Commission is responsible under Art. 61(2c) of the ECAC for determining whether end-to-end connectivity between end-users is threatened. Specifically, BEREC (Body of European Regulators for Electronic Communications) is responsible under Art. 61 para. 2c "DETEC" to inform the European Commission whether end-to-end connectivity between end-users is threatened. Some national and pan-European services are calling for a European force in the standardisation process. Only Europe-wide solutions would make sense and the EU Commission could exert corresponding pressure. One addressee stresses that other public institutions could also participate in the technical standardisation process, whereby most of the technical input must come from industry and the technical discussion must take place primarily between the market participants. A few messenger and video services mention **national authorities**, which have the local market knowledge and can call on national market players to participate in the discussion.

Significantly more respondents point to the market participants - i.e. the **industry** - as necessary participants in the standardisation process, which ultimately corresponds to the established procedure. The industry should form a working group - according to a well-known open source service - as it should be left to the industry to develop a standard. The market players would be the ones who developed and deployed the technologies. They would know the challenges and implement the standard in the end. However, they would have to speak with a unified voice and make clear what makes sense and what does not. The desire for market participants to participate reflects the diversity of the industry. Market participants should ensure that all regions as well as large and small industry players would be represented. One respondent stresses that the **negotiations should be open to all market participants**. Other organisations mentioned include the XSF (XMPP Standards Foundation), which supports protocol extensions for XMPP, the W3C (World Wide Web Consortium), which developed the WebRTC standard, and the Matrix.org Foundation.

In the meantime, an interoperability regime has been adopted at European level - as described - in the DMA. The opinions and comments expressed by the industry will therefore be discussed with the

[288] The responses evaluated here were recorded by the Bundeskartellamt in summer 2021, well before the trilogue agreement on the DMA in March 2022.

The results are compared with the adopted solution and the expectations for future market development.

IV. Conclusion and conclusions

In this report, the Bundeskartellamt examines the key question of how the level of data protection in Germany can be improved. A special role is played by the **effects interoperability** could have on the **level of data protection.** Expectations have been expressed on various occasions that interoperability could make it easier for consumers to switch to privacy-friendly messenger services and thus promote the quality of data protection in this area. Other objectives related to interoperability, such as ensuring connectivity in the area of interpersonal communications or reducing the market power of leading messenger services, were not directly addressed by the enquiry.

The Bundeskartellamt had already emphasised in the interim report that political measures and legal requirements can have very different effects on the companies and applications concerned due to the **heterogeneity of the industry.** This results in requirements for any regulatory or legislative measures aimed at eliminating problematic situations. Not only should these be taken into account, but also **opportunities for further market development** should be **preserved** (see 1.). Last year, the German Federal Cartel Office (Bundeskartellamt) conducted a sentiment survey on interoperability and the impact on the level of data protection in 2021. After the German legislator with Section 19a of the ARC also enables prohibitions with regard to lack of interoperability vis-à-vis its addressees, an **interoperability obligation for** the "gatekeepers" of the industry of messenger and video services has now been initiated at the European level in the Digital Markets Act. First of all, it is stated that measures to improve the level of data protection for individual services should keep the competitive development of the industry as a whole in mind. Overall economic effects should be taken into account. Then it is examined how the opinions expressed in advance by the industry and the current legislative plans compare (see 2). Next, the focus is on the impact of interoperability on data protection and the associated data security efforts. Again, it is the behaviour and decisions of consumers that have a decisive influence on the evaluation (see 3).

1. Exploit potential, avoid collateral damage

The investigations have painted a diverse picture of the industry. This does not only concern the different use and application of technical criteria such as protocols, servers,

encryption or identifiers, which are decisive for the data security and data protection of a messenger. Furthermore, the services also differ in terms of their functions, their business models and their economic significance. The spectrum of industry participants goes far beyond the well-known and widespread messenger and video services.

International diversified groups with a **broad technological or digital spectrum** are active in the industry of messenger and video services with high turnovers. This concerns not only WhatsApp and Facebook Messenger, which belong to the digital group Meta, but also the technology groups Cisco with Webex and also other digital groups such as Alphabet (Google) with Google Meet and Google Chat[289] as well as Microsoft (Teams, Skype), each with considerable positions of power, especially in operating systems for mobile and conventional applications. Many leading messenger and video services thus not only have considerable know-how, but also strong positions in areas that are important for the "messaging" and "video conferencing" functions. In addition, there are large corporations that have their focus abroad, such as the Japanese Line Corporation, which belongs to the powerful and diversified South Korean Naver Corporation, which successfully operates a search engine, or WeChat as part of the Chinese state power, which are less present on the German market but no less successful than the dominant companies here.

Not surprisingly, this phalanx of heavyweights blocks the view of the other industry members. Yet some other services have found their place in the industry and operate **sustainable business models**. They may seem "small" compared to the big players in the industry, but on their own they are generating quite remarkable, stable revenues with the intention of continuing operations. These are, for example, national services or services concentrated on German-speaking regions, services that advertise special data protection quality or focus on certain functions (e.g. webinars) as well as many paid open source services or clients that are based on open source services as well as free and unpaid applications that enjoy great popularity, e.g. in the education sector or among expert users.

As a result, "messaging" and "videoconferencing" is a global business and an industry that generates **technological and digital developments and innovations** not only on the part of the larger participants. Competing services are characterised by innovative business models and specialisations based on particular services and functions, and not

[289] Google Chat was not included in the investigation because, according to *Google*, the service was just starting up at the beginning of the sector enquiry.

only on the part of the free systems and applications is there a **lot of expertise and commitment in terms of independence and protection of users' personal data**. However, the state of the market suggests that this potential has so far not been exploited, not been distributed across the board and not been used in favour of a high level of data protection as it could be.

In the investigations, the view has been expressed from various sides that better results would also have been achieved in data protection if **international and open standards had** been used from the beginning. But that was not the case. Developments have taken a different course and this reality must now be dealt with. Individual industry representatives have used the opportunity to develop a closed business model, which on the one hand is particularly attractive to consumers due to the new types of communication possibilities and the fact that it is free of charge, but on the other hand can produce undesirable results with regard to data protection.

But the reality is also - the sector enquiry has revealed it - that many other business models have developed alongside them, which apparently work well nonetheless. These business models are also a reflection of **consumer desires**. So the wheel cannot simply be turned back to eliminate undesirable effects. In the case of any legislative or regulatory measures aimed at dissolving the power positions and to be carried out on behalf of consumers in favour of the protection of their personal data, it must be examined whether other business models are at risk of being affected in the process.

If interoperability is introduced as such a measure, it is not only the necessary investments in technical changes to the services or the development of technical innovations for implementation that must be taken into account. Also to be taken into account are possible positive or negative welfare effects through **changed incentives for innovation and effects on business strategies and the intensity of competition, especially of the market participants who compete with the leading services**. The analysis of the interdependencies especially around the topic of interoperability is thus multi-layered and complex. With the introduction of § 19a of the Act against Restraints of Competition, the German legislator has taken an important step. At the European level, the path was continued and is now leading to the Digital Markets Act, which can also mean changes for messenger and video services.

2. The future reference offers according to the DMA - a framework for the mood?

In the summer of 2021, the Bundeskartellamt published a "mood survey" on interoperability issues. determined. The obligation of gatekeepers to interoperability contained in the DMA was at that time in

not yet known in this form. The replies of the messenger and video services rather referred to an interoperability concept which had not been defined in more detail by the Bundeskartellamt in order to avoid pre-determinations and controlled expressions of opinion. The concept of an interoperability obligation standardised in Art. 7 DMA provides for limits under three aspects.
First of all - following the overall concept of the DMA - only designated gatekeepers among the messenger services are addressees of the obligation. Furthermore, the obligation only comes to life as soon as another service (voluntarily) approaches the gatekeeper with a corresponding petition. Finally, only the basic functions are covered by the obligation.
Overall, the survey showed that interoperability is not rejected outright by the companies concerned. Furthermore, the answers revealed that **accessibility across service boundaries** is **already possible to a certain extent.** For example, the free messenger clients are fully interoperable within their system. There is also a wide open source area that pursues interoperability as a business model. With some video services, at least accessibility is also made possible for third party users, for example by sending invitation links. Especially for the business customer sector, there are also bilateral regulations or interoperability agreements as well as service providers who can establish mutual accessibility. Finally, a very rudimentary form of connection is offered by multi-messengers, with the help of which users can operate various messenger services via a software interface and read content.
Just under half of the companies surveyed had shown themselves **open to voluntary interoperability projects**, although - asymmetrically to this - only less than half would participate. With these figures it had to be taken into account that the respondents had provided their assessment for or against voluntary interoperability in each case with numerous comments, preconditions, references and restrictions, as the interoperability concept had not been specified in more detail by the Federal Cartel Office. However, this had been accompanied by the clear position of a large part of the industry that a **legal obligation for interoperability** is **not desirable.** In the case of enforced interoperability, the companies with a negative stance had feared in particular negative effects on innovation activity and thus also on the level of data security and data protection in messaging and audio/video exchange.
The regulations in the **DMA** take up some of these aspects. They provide for an asymmetric interoperability obligation in Art. 7. The DMA thus requires more than a voluntary agreement, but restricts the obligation to designated messenger and video services of companies previously classified as gatekeepers and links the obligation to a corresponding application. The implementation of the reference offer to be made by the gatekeeper is thus likely to be only the

Messenger and video services, which are classified as number-independent interpersonal communication services. In the Bundeskartellamt's investigations, one fifth of the respondents had named industry participants which they thought should be subject to an obligation. These were services leading in terms of turnover or user numbers, which at least in principle comes close to the criteria for the definition of a gatekeeper.

The DMA's interoperability commitment covers **basic functionalities** including the sending of all files, initially text messages and voice calls, then group chats after a period of two years and finally video calls after a total of four years.

Three quarters of a year before the trilogue agreement in March 2022, many messenger and video services had expressed their support to the Bundeskartellamt for a narrow interoperability model consisting of text messages, which leaves room for innovation in other functions and minimises switching efforts. However, a package of interoperable functions was only considered useful by some services if text, audio, video and content exchanges are included. Here, too, basic agreements are thus recognisable, if the DMA also provides for a time staggering here. Video telephony is only to be made interoperable four years after the designation of the respective service.

The messenger and video services interviewed by the Bundeskartellamt could only imagine implementing interoperability on the basis of **global technical standards.** So far, technical principles (for interoperability) have been developed in a global context in standardisation bodies. The industry had said that otherwise it would be very costly to have to meet different requirements worldwide and offer different sets of interoperable functions.

It remains to be seen to what extent this aspect will be included in the possibilities opened up by the DMA for the Commission to regulate details in implementing provisions or delegated acts (Art. 46 para. 1, Art. 12 para. 4 DMA).

Art. 7 (3) DMA requires gatekeepers to maintain the level of security offered to their own end customers, including end-to-end encryption if necessary, for all interoperable services. As already explained, the services largely use individualised protocols and encryption techniques. This also applies to end-to-end encryption. It is subject to technical limitations and is used by some services - regardless of this - only for certain functions. Some large services do not yet use it. It often has to be activated by the users or hosts. **Difficulties in implementation and possibly declining security standards** are to be expected here, unless the **state of the art can be** established.

In general, the type of technical implementation of interoperability is not yet described in detail. The gatekeeper is only required to provide the necessary technical interfaces or comparable solutions. In the Bundeskartellamt's survey, most services spoke out in favour of implementing interoperability via **server interfaces**, although alternative methods were only close behind in the ranking.[290]
It remains to be seen which regulations will (have to) be made here. This will also depend on whether and to what extent the respective reference offers of the gatekeepers concerned are demanded by the messenger and video services, i.e. corresponding applications for the establishment of interoperability are made.

3. Data protection under interoperability between theory and real challenge

With regard to the concrete effects of interoperability on data security and thus on the level of data protection, the assessment of messenger and video services expressed in the Bundeskartellamt's survey was multi-layered: on the one hand, the argumentation already mentioned at the beginning was put forward: services promise themselves new possibilities if accessibility or large numbers of users no longer represent a differentiating feature. This could be associated with a revival of the intensity of competition. Consumers could switch to more data protection-friendly providers if services were accessible to each other, **data protection** could **thus** become **more important as a competitive advantage** and the overall level of data protection could increase.
On the other hand, the companies surveyed had also predicted indirect (negative) effects on data security and data protection. For example, a possible interoperability obligation could have a **dampening** effect **on the innovation activities of** providers and subsequently also for the level of data protection, especially if globally uniform standards or protocols that lag behind existing standards in encryption as well as identifiers based on the lowest common denominator would have to be used. **Increasing data security requirements** could ultimately lead to higher costs, which are a hurdle for smaller providers in particular

---

[290] On technical options for implementing end-to-end encryption under interoperability, see also *Bundesnetzagentur*, "Interoperability between Messaging Services - Secure Implementation of Encryption", April 2023, available at: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteropEncryption.pdf?__blob=publicationFile&v=1. The study involves seven messenger and video services and is based on an examination of publicly available technical documentation and scientific publications.

could. The technical integration is likely to cause a **lot of effort**, especially if the messenger systems involved themselves operate an architecture consisting of different servers on which different functions and services are located.

The interviewees were relatively unanimous that interoperability that is mandatory by law would make it more complicated to guarantee the security of data and thus also to comply with data protection laws. Some voices in the industry countered that the difficulties with data security and data protection could be solved on a technical level; ultimately, it was all a **question of willingness to invest**. In any case, the majority of the messenger and video services surveyed did not expect a higher level of data protection from enforced interoperability. On the contrary, some emphasised that the **lower limit for the level of data protection** is set by the applicable data protection laws, such as the General Data Protection Regulation (GDPR). These would have to be complied with, regardless of whether there was interoperability with other messenger and video services or not.

The Bundeskartellamt agrees with many voices from the industry that interoperability will place **new demands on data security and data protection.** Essentially, it is not only questionable what identity management might look like. The BSI has already noted that extensions would have to be made to the network infrastructure of the messenger servers - e.g. to the Domain Name System (DNS).[291] The messenger and video services use different identifiers, but the telephone number - as the results of the investigation have shown (see D.II.2) - is definitely used less than initially assumed. However, it leads to the next question, namely how to deal with users' contacts, including those of users of other messaging systems, if applicable, under interoperability.

It is also still open how quickly **the problems with end-to-end encryption** in groups can be solved, possibly via the MLS standard or possible other further developments of the IETF working group MIMI. This will depend on the extent to which the services can and want to implement the standard and open source implementations. At the moment, messaging systems are largely based on individual protocols. Even if many go back to a common basis - the double ratchet protocol - the corresponding individualisations are sufficient to prevent interoperable end-to-end encryption.

---

[291] *BSI*, Moderne Messenger - heute verschlüsselt, morgen interoperabel?, November 2021, p. 10, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

The very different network architecture of the messenger and video services - as revealed in the investigations - is also challenging, especially when functions are assigned to different servers or **federated systems in** general are to be made **interoperable with each other.** According to the BSI, the topic of federation, i.e. cross-server communication, is becoming more tangible with the MLS standard, even if the development of concepts is still in its infancy and there are only a few practical, cryptographically secure approaches to solutions. In the course of the investigations, Element (Matrix) also pointed out in the summer of 2022 that the standard in its current form unfortunately cannot support complete interoperability, as decentralised and federated networks are not fully supported. The MLS protocol would have to be extended for this purpose. In the meantime, the IETF has announced that the work on the MLS standard has been completed. Matrix also plans to use it.[292]
Finally, numerous questions arise from the field of data processing. For example, the aspect of **(meta-) data monitoring and responsibility is** critical when users' personal data pass through even more hands under interoperability. The fact that some services upload contact directories and others do not has yet to be resolved for the users concerned.
As noted in this report, **legally compliant data storage** is a challenge and requirement for some services to meet. Interoperability increases the likelihood that different jurisdictions will be affected.
The **classification and evaluation of these difficulties, especially from a macroeconomic perspective,** and the possible emergence of further challenges depends on the development scenario that is taken as a basis. I.e. either the real conditions can be taken into account, where the industry-wide interest in interoperability seems to be moderate. Or a market-wide interoperability regime can be assumed, in the course of which far-reaching standardisations would have to be implemented. However, this perspective seems more theoretically interesting at present, e.g. as a reference scenario for the cost-benefit analysis of the measures that will actually be taken in the future. Finally, an assessment is made more difficult by the fact that the exact technical implementation of interoperability by the gatekeepers to be named in the DMA is still open.

---

[292] Cf. *IETF*, Messaging Layer Security: Secure and Usable End-to-End Encryption, available at: https://www.ietf.org/blog/mls-secure-and-usable-end-to-end-encryption/ and *Golem*, IETF standardises protocol for secure group chats, available at: https://www.golem.de/news/messaging-layer-security- ietf-standardisiert-protokoll-fuer-sichere-gruppenchats-2303-173089.html.

but this will be a major determinant of data security, data protection and the necessary investments in the same.

In the Bundeskartellamt's view, the **actual current initial situation** does not lead to the expectation that the messenger and video services sector will interoperate with each other within a very short time. It will ultimately depend on the wishes of the users of the respective services whether the respective interoperable reference offer will be demanded or not. The Bundeskartellamt continues to consider the attitude of **consumers towards** interoperability to be a **variable that is difficult to assess**: whether a noticeably large number of consumers would actually switch to data protection-friendly providers in the event of interoperability, as is hoped for in various cases, can at best be described as open and rather questionable, according to current surveys by the Federal Network Agency[293] and the Federation of German Consumer Organisations[294] on user interests and willingness to switch. It is also possible that consumers would not react significantly to the interoperability of messenger and video services, as they are satisfied with their current multi-homing solutions and use them even more intensively.

According to feedback from the market, the **greatest hope** could be to make it possible to **switch entire consumer groups,** such as those found in sports clubs, so that the individual user is spared the tedious task of convincing contacts. In the course of a start-up project, it was made clear to the Federal Cartel Office that there is obviously interest at club level in Germany in turning to data protection-friendly messengers and even developing their own service. The **connection to the WhatsApp messaging system** was described as an essential factor for the success of such a project. Ideally, the gatekeepers themselves should design complete interoperability with other messenger services, but in any case at least make their APIs freely accessible so that smaller providers can develop interoperable solutions. In the Bundeskartellamt's investigations, many free messenger clients and open source services also pointed out that consumers would be able to switch if there were access to the leading services. Increasing user numbers were expected. In the course of the

---

[293] *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, May 2020, available at: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf? blob= publicationFile.

[294] *VZBV*, Interoperability in Messenger Services, May 2021, available at: https://www.vzbv.de/pressemitteilungen/messenger-dienste-regulierung-mit-augenmass.

The access obligation in the DMA would now at least have the chance to prove this thesis.
"revitalise", i.e. make it easier for new entrants or competitors to enter and consumers to
consumers to make the switch.
Provided there were only isolated applications for **bilateral interoperability agreements,** the problems would seem to be solvable and the necessary investments acceptable. Solutions are planned via interfaces, which are already practised in this basic form in the market by some messenger and video services. The restriction to the basic functionalities envisaged in the DMA is a construction through which **differentiation possibilities** - at least theoretically - can basically be preserved for the services. On the part of the services, it will then have to be looked at individually in concrete terms whether and to what extent the technical conception of the services, which - as described in Chapter D.I.1 - is very different, can guarantee a corresponding separation into interoperable and other functions.
For consumers, the DMA interoperability obligation represents, in addition to the
Multi - homing on the one hand represents another possibility to reach users of other messenger services. With the help of the DMA regulation, they could, in principle, be less dependent on leading services for group communication, which have so far profited from network effects. On the other hand, the extent to which - as claimed by services popular with consumers - the **user experience will be restricted** and the **attractiveness of the product will decline** - cannot be estimated at this point and depends on many factors. First of all, on whether - as described above - the consumers will appreciate interoperability.
and accordingly "mandate" their services to request a reference offer or the services promise themselves new business opportunities. Furthermore, the sector is likely to evolve. One is the implementation of new features for users. If new features catch on quickly, the interoperable product may actually lose its appeal. This in turn depends on the appreciation and preferences of consumers. Whether they find it more important to communicate with users of other services and would limit their messaging to interoperable features or whether they prefer to multi-home and use the full variety of messaging features at any given time cannot be clearly answered at this time. According to the DMA's **timetable for the implementation of the reference offer,** video telephony interoperability will only be required in four years' time, which seems a rather long period in a dynamic market. Admittedly, this point was not disregarded insofar as corresponding changes to the reference offer and the implemented deadlines can be made by the legislative side. However, such a **long implementation and thus also forecasting period makes it** difficult to make serious statements about the suitability of the measure. On the other hand, the

technological development opens up new possibilities and possibly solutions, such as the MLS standard for end-to-end encryption of group communication or the newly established MIMI working group of the IETF, which is also conducive to any interoperability efforts.

If - contrary to expectations - gatekeepers had to implement a large number of individual solutions, the above-mentioned difficulties for data protection and the overall economic cost-benefit calculation would increasingly come into the limelight. Here, a multitude of individual solutions is likely to be disadvantageous from a macroeconomic point of view and an **industry-wide standardised regime will be** necessary.[295] Due to the diversity of the industry, the many different business models that are not based on personalised advertising and the different technical starting points as well as the complex consumer wishes, further discussion with the industry can then be expected. Based on the results of the sector enquiry, in the Bundeskartellamt's view, an **interpretation that protects innovation and investment and** leaves room for technological development should be encouraged for any regulatory dialogue with the appropriate leeway.

[295] Similar considerations are made by the authors of the BNetzA study "Interoperability between Messaging Services - Secure Implementation of Encryption", April 2023, who examine different options for a possible implementation of end-to-end encryption under interoperability, available at: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteropEncryption.pdf? blob=publicationFile&v=1.

G. Approaches for more competitive data protection

In the preceding chapters, the Bundeskartellamt has dealt intensively with the concrete security features and practices of data processing in messenger and video services, consumer law infringements of the services as well as the practical relevance of legal measures by the legislator - data portability and currently interoperability - for consumers' everyday messaging.
As a result, the impression arises that the quality of data protection, especially on the part of consumers as demanders, and also in the case of some services, does not receive the necessary attention within competitive selection processes, so that the level of data protection would improve in a market-driven manner under the given framework conditions.
This chapter now focuses on how the level of data protection in Germany could be improved in a timely manner. In its questionnaire, the Bundeskartellamt asked the messenger and video services to express their views on this (see I.). Against the background of the results of this investigation, the Bundeskartellamt has taken up some aspects which could lend greater weight to data protection in competitive processes (see II.). Finally, with the rating, an instrument is presented and discussed which seems suitable to motivate both the services offering and the consumers requesting them to understand data protection as a competition parameter (see III.).

I. Investigation results

The Bundeskartellamt asked the messenger and video services to choose which measures could improve the level of data protection in Germany. The broadest approval on the part of the services was found in the categories specified by the Bundeskartellamt "public promotion of open source projects" (45%), the "use of data protection-friendly services in the public sector" (41%), the "education of consumers" (45%) and the "better enforcement of data protection law" (43%). Many services commented enthusiastically on these measures. The measures "standardisation", "data protection audits for providers" and "measures of the
Competition supervision" met with less approval in relation to this.
Some **leading providers** said that further **measures in favour of data protection** were not necessary. There is already a high level of data protection in messenger and video services in Germany, especially when dealing with business applications. A service that is popular with consumers emphasises that it already provides its German users with a sufficient level of data protection measures. Its own vision is to connect the world privately. They are committed to data protection and data security, as stated in the answers to this questionnaire. One

strives to be open and transparent about the personal data that is collected in order to provide the service to German users and to make it secure. Information on this would be available on the website. Other major services point to a lack of market knowledge for Germany or a lack of reason to deal with it.

1. Promotion of open source and standardisation

There is broad support for public funding of open source projects in all provider groups. This refers on the one hand to the promotion through public funding, but also through the use of open source services in the public sector.

Various free services have made more detailed comments on this: as long as the market is dominated by companies that earn money with their users' data, the **level of data protection will** suffer. Open source projects with public funding could challenge this status quo and offer users alternative services. The more open source is promoted, the greater the pressure on established American-based providers. Another service points out that if you can't develop everything yourself, **financially pooling your efforts and investing in** open source projects is one way to stay competitive with more developed competitors. Many problems with messengers and communication in general are also due to **commercial interests** and the resulting various constraints, so that users cannot easily leave the corresponding systems. The choice of provider is no longer completely free and a change of provider is associated with increased effort for the user. As a rule, free messenger systems have a higher level of data protection, as they are not influenced by economic interests. Users who were concerned about data security and data protection would have more choice among free messenger clients.

Several competitors of the large messenger and video services state that the promotion of open source does not only refer to data protection-friendly free offers. According to various services, it should also include the **promotion of products from innovative competitors of** the established services. Open source is not synonymous with "free". Open source software is the only way to generate **trust in the functionality and security of** software and to achieve rapid market penetration and more flexibility. Thus, business models had already emerged that were not based on violations of data protection law vis-à-vis consumers.

Another competitor of established services goes on to say that open source projects emancipate customers: They could look into the software and thus check it objectively,

whether promises were actually built in. Should the software no longer be developed, customers could commission others to do it, which would protect their investment in the original solution. Special features could also be realised that one might not have thought of oneself. And last but not least, one sees a **security gain for** all if independent experts can inspect the code and point out problems. Public funding should primarily be given to systems that are "sustainable". The promotion of projects that already comply with existing **(international) standards** and the promotion of related open source projects (or the commissioning of closed source projects that support public interfaces) contribute significantly to such "sustainability". Even if the companies/developers involved no longer work on a project, the source code is still freely available and other developers can take over the code and develop it further (for example, even with public funding). This means that all changes (whether publicly or privately funded) would always benefit the general public and no public money would flow into private companies or projects, where it would peter out and no "sustainable public good" would emerge. If such a company disappeared from the scene, the money invested would be irretrievably lost, unlike in the case of open source software. Public standards and the promotion of the development of open

Source projects are essential for a free, sustainable and independent society.

US services also agree. Promoting open source projects together with standardisation is the best and most effective way to **drive innovation**.

In general, one third of the respondents consider **standardisation to** be suitable for achieving a better level of data protection. It enables interoperability. Open standards could be viewed and commented on by a large number of people. Problems with data protection and data security could thus be found quickly. In addition, economic interests of service providers would usually be weighted less, as people without economic interests could also participate in the standardisation process. Standardisation would create more competition, which is basically positive. It would also mean that data would no longer be only in the hands of the three largest providers. Product development would become easier and less risky and in the end less costly.

2. Use of privacy-friendly services in the public sector

Many messenger and video services point to a possible **role model function of the public sector. The** use of non-privacy-compliant messengers is still widespread among both public authorities and companies. If non-privacy-friendly services are used in public

If these services are used in other areas, this gives them increased legitimacy from the users' point of view.

Users should be able to choose a self-determined path for their communication with the authorities without passing on their data to third parties. For example, it would also be possible for public authorities to operate their own XMPP servers and thus maintain or obtain full data sovereignty. Many universities, for example the HU Berlin, already operate such systems.[296] Public institutions should pursue an "**open source first" approach in their tenders in order** to be able to account for the use of public funds).

It goes on to say that open source should become obligatory for the public sector. This does not mean that free projects should be created, but that taxpayers' money should be **invested** in **solutions from innovative German companies.** Ideally, the **government should buy working solutions and use them itself**. This would lead to the creation and improvement of competitive products. He is sceptical about government funding in general, but if governments buy products to promote and stimulate technologies, this is more effective than simply handing out money to those who can write the best proposal.

Another competitor of the established services explains that funding can usually be more of a burden than a help for developing companies in Germany - especially if the company concerned has experts for its projects and no experts for funding and lobbying in its ranks. The difficulties begin with finding a suitable funding programme, continue with a great deal of bureaucracy in the application process, and extend all the way to severely **restrictive funding conditions**. The situation is similar with tenders. For example, they would have liked to take part in a call for tenders from a state ministry for a school fair. participated. This failed due to "artificial limits". The **framework conditions of the tenders** - e.g. requirements for minimum turnover - could not have been met even by established companies.

It would make more sense to support state or local authorities if they use open-source products from innovative German companies. **Companies would always be better served by realised turnover than by subsidies**. The country's own talents should be made visible and the domestic IT sector should be promoted. Digital technologies would be systemically relevant. One should not make oneself dependent on corporations, which could be influenced by a variety of uncertain factors. The

[296] See *HU Berlin*, available at: https://www.cms.hu-berlin.de/de/dl/kommunikation/chat.

Today, the open source world offers solutions for all applications that are no less good than the mass-produced products of a few monopolists. And where there is still a need, every German developer, every German IT company will be happy to support when the customer calls.
Finally, the investigation referred to the **education sector**. Teachers and parents or, in higher grades, teachers and students often still communicated in groups via popular widely used messenger services. A leading video service is also often used for home schooling. In addition, large digital and IT companies are investing heavily in this area in order to bind teachers and thus students to their own software - and this of course includes messaging apps - at an early stage.[297]

3. Consumer education

Consumer education is an important aspect of a future data protection strategy for all service groups. This view is held across the industry.
Consumers must continue to be sensitised to the topic of data protection. It is part of the development of **media competence**. At present, the task of informing users about the dangers of unencrypted communication is almost exclusively left to **civil society,** while the government keeps calling for the breaking of end-to-end encryption. Knowledge about data protection and trustworthy IT systems as part of media competence is even lacking among many teachers.
Communicating the importance of data protection to consumers would, according to two major services, lead to consumers valuing data protection more and choosing the appropriate offers, which in turn would be an incentive for competitors to offer more data protection-friendly products.
One service objects that consumer education already takes place to a sufficient extent, but has only limited effects due to **centralised market power of individual companies.** Another service argues similarly. Users should really have a choice and be able to make this decision themselves and freely, which they currently cannot do. One example is the questionnaire of the Federal Cartel Office, which is a Microsoft Word document.
An open source service proposes a **privacy rating.** Most consumers would not be able to properly comprehend data protection issues and would mostly

[297] The keywords are free professional development programmes of the digital corporations for teachers who use the corporations' own products for teaching and learning. The teachers fulfilled the function of brand ambassadors, so to speak.

also not read the privacy statements. A rating would lead to competitive resonance in the market, as no messenger or video service would want to lose users because of a worse rating compared to its competitors.

4. Further investigation results

Some messenger and video services also commented on "better enforcement of the data protection law", "competition supervision measures" and "data protection audits for providers".
On the question of **enforcement of data protection law**, one service commented that Corona had shown how toothless the data protection tiger really is. The fact that Zoom is used in so many companies does not speak for the enforcement of data protection. Another service said that even if "AVV[298] and co" were concluded with the company, the use of the Cloud Act[299] might expose the data to American authorities. One video service says that effective enforcement of regulations, such as the Cloud Act, will hurt large companies. However, the laws would also be difficult for smaller companies to implement, which should not be underestimated. What matters, he says, is good execution.
Data protection violations by various service providers (especially from the USA) were widely suspected, but **inadequately prosecuted** by data protection authorities, among other things because of the competence of the overburdened Irish authorities. American "chat system providers" are not sufficiently controlled.
One open source service says that Germany already has strong data protection laws. If a data protection incident were to occur with a messenger or video service, the data protection authorities would probably already have the tools to solve the problem. Another provider expressed a similar opinion. The **GDPR is** a "high water mark" and a world leader in terms of efficient and proportionate data protection law based on principles.
A US service says enforcement of the GDPR by member state data protection authorities has been patchy and has led to skewed results in the internal market. It is

[298] According to the GDPR, every company that has personal data processed on its behalf - i.e. by a service provider - must conclude a contract processing agreement.

[299] The Cloud Act (Clarifying Lawful Overseas Use of Data Act) is a US law that has been in place since 2018 to allow US authorities access to stored data on the internet. The law obliges American internet companies and IT service providers to guarantee US authorities access to stored data even if the storage does not take place in the USA, see *Wikipedia*, available at: https://de.wikipedia.org/wiki/CLOUD_Act.

clear that some of the largest providers had looked to the EU for a more lenient "main establishment regime". The role of the European Data Protection Board[300] is to ensure adequate enforcement standards in the internal market. For example, restructuring the European Data Protection Board into a real enforcement authority could be helpful in improving enforcement standards within the EU. The European Data Protection Board and the data protection authorities of the member states should also seek ways to ensure that privacy by design principles are implemented as good practice in the industry. This could be implemented via binding guidelines - based on the core principles of the GDPR - and prevent abusive / dominant companies from using manipulative design practices to gain unfair access to users' data. As examples, the British ICO
"age appropriate design code (children's code)"[301] and that of the "Australian eSafety Commissioner's

[300] The European Data Protection Board (EDSA) is an independent European body that aims to contribute to the consistent application of data protection rules throughout the European Union and to promote cooperation between EU data protection authorities. EDSA consists of representatives of national data protection authorities and the European Data Protection Supervisor (EDPS). EDSA can issue general guidance to provide clarity on the terms used in European data protection laws for the purposes of consistent interpretation, especially for a wide range of stakeholders. To ensure uniform application, it also has the power to issue binding decisions for national data protection authorities, cf. *EDPB*, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_de.

[301] The 'Children's Code' (or the Code of Age Appropriate Design) was issued by the UK Information Commissioner's Office (ICO) and came into force in September 2021. It sets out 15 standards that online services must follow. This ensures that they meet their data protection obligations to protect children's data online.
comply. The Code applies to "information society services that children can access, i.e. most for-profit online services, such as apps, search engines, social media platforms, messenger services or internet-based voice telephony services; The Code applies to companies based in the UK and companies outside the UK that process children's personal data in the UK, see e.g. *ICO*, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age- appropriate-design-code/.

Office safety-by-design code"[302] . Both would be mandatory, legally binding design codes based on applicable laws and regulations.

One interviewee comments on fines. If **fines** were to be imposed, they would have to be such that they would also trigger a change in repeat offenders. If consumers were really harmed by data protection breaches, fines could become a smaller part of a larger set of instruments. A distinction should also be made between negligible breaches (negligent company that did not pay attention) and nationwide sophisticated breaches when imposing penalties.

A good quarter of the services surveyed address **measures of competition supervision**. All services commenting here object to the strong market position of individual services and their behaviour. These services would have used the global availability of the internet to build up monopoly structures and to disregard national jurisdiction. Dominant companies should not be able to gain competitive advantages because of "underperformance" in data protection. In the centralised market for messenger services, the big players dictate anti-privacy terms of use to their users and prevent them from switching. This comes close to abusive behaviour of market power and the authorities should take measures to force the opening of the markets. Companies with market power would prevent third parties from communicating with users of their service. This would leave innovative, more privacy-friendly systems with little opportunity to position themselves in the market. According to one service, a separation of message transport and apps should be thoroughly examined.

Data protection audits for providers receive less attention among respondents. One service states that it would definitely be helpful if the government carried out such audits, especially if the results were published. One example, he says, is the audits of official food monitoring in Baden-Württemberg.[303] Another service points out two aspects: Mandatory audits for foreign services might be difficult to implement. Voluntary audits could raise the public profile of privacy-friendly services, but would mainly affect competition between services.

---

[302] A model for industry participants of all sizes and maturity levels that provides guidance on how to incorporate, assess and improve user safety. The principles make user safety a fundamental design consideration (Source: Australian eSafety Commissioner).

[303] See *MLR Baden Württemberg*, available at: https://verbraucherinfo.ua-bw.de/lmk.asp?ref=3.

privacy-friendly providers, while market-strong providers simply did not conduct a voluntary audit if it could be expected that the result would not be positive.
From the measures on which the services commented, the Bundeskartellamt subjected those that met with the most approval to a closer analysis (see the following chapters). They are part of a strategy to increase the importance of data protection as a differentiating feature or selection criterion in competition, both on the part of the services offering it and on the part of the consumers requesting it.

II. Data protection as a competitive parameter

In the following, we will first discuss how data protection could be promoted on the supply side - in the services. Are there starting points that promise success in the short term (see 1.)? Subsequently, the question is whether and how measures must be designed so that consumers as demanders switch to data protection-friendly services, despite a disadvantageous information gap, which has so far worked in favour of players with high accessibility and a free offer. Contributions from academia will be presented on this, which can provide guidance for the selection of measures (see 2.).

1. Strengthening data protection-friendly services (supply side)

In the investigations, many messenger services commented on how privacy-friendly messenger and video services could be strengthened. One aspect was the promotion of open source and standardisation, where improvements were desired. Another starting point was the use of privacy-friendly services - not only privacy-friendly open source applications, but also other privacy-friendly services - in the public sector. This is linked to the hope of achieving a higher level of acceptance of less well-known data protection-friendly applications in other private sector areas as well.
In researching current funding opportunities, the Bundeskartellamt came across only a few targeted funding programmes for free applications, small companies or start-ups - beyond the major funding programmes. Worth mentioning are the EU Commission's Open Source Software Strategy 2020- 2023 under the motto "Think Open" and the BMBF's "Software Sprint" for
"innovative individual projects by creative thought leaders (free programmers) in the areas of civic tech, data literacy, open data and open source". The Bundeskartellamt has therefore asked messenger and video services that have made more detailed statements on the promotion of open source for further explanations on the subject.
According to industry representatives, the most important organisation in Europe in the field of promoting open source - communication software is the "NLnet Foundation", in particular in cooperation with

with the "Next Generation Internet Initiative"[304] of the European Commission and the "Prototype Fund"[305] of the Federal Ministry of Education and Research.[306]

The **NLnet Foundation** supports organisations and people who contribute to an open information society. It was instrumental in spreading the internet across Europe in the 1980s. [307] The European Commission has launched the **Next Generation Internet Initiative (NGI)** to fund and support talented researchers and innovators to develop the technologies needed for tomorrow's Internet. In particular, this involves open source solutions that offer trust, privacy, security and inclusion, as well as a European open source alternative to commercial off-the-shelf products.[308] "The good thing about such tools," says the European Commission, "is that end-users have full control over them, and at the same time they protect our data, so that we can discuss anything that is confidential for our business or intimate for our family. Even if the internet connection is interrupted, these apps do not rely on a connection to a single provider, and many of them can be used on our end-user devices without the need for a connection to the internet.

be carried out without interruption"[309] . Some of the services surveyed by the FCO - BigBlueButton, Conversations, DeltaChat, Dino, Meet.jit.si - have received funding from the organisation.[310] The XSF describes the funding platform as popular and comparatively easy to access, as

---

[304] After the first year of the project, the first developments are now available that offer trust, privacy, security and inclusion, as well as a European open source alternative to commercial off-the-shelf products.

[305] See *Prototype Fund*, available at: https://prototypefund.de/.

[306] Finally, the "Google Summer of Code" is worth mentioning. This is an annual programming scholarship organised by Google and not a long-term support programme. Nevertheless, industry representatives describe it as a helpful programme in which they have already participated several times. See *Google*, available at: https://summerofcode.withgoogle.com/ and *Wikipedia*, available at: https://de.wikipedia.org/wiki/ Google_Summer_of_Code.

[307] Cf. *NLnet Foundation*, available at: https://nlnet.nl/ and https://de.wikibrief.org/wiki/NLnet.

[308] Cf. *Next Generation Internet*, available at: https://www.ngi.eu/about/.

[309] Cf. *Next Generation Internet*: People-centred technologies in times of crisis, available at: https://ngi.eu/wp-content/uploads/sites/48/2020/04/NGI4ALL_NGI-for-COViD19_DEU.pdf.

[310] A list of currently funded projects can be found at *NLnet Foundation* https://nlnet.nl/project/current.html.

it distinguishes itself by also donating small amounts of funding. It "could be an example for (another) German funding platform".

The **Prototype Fund** is a project of the Open Knowledge Foundation[311] Germany, funded by the Federal Ministry of Education and Research (BMBF). Funding is provided to developers from civil society "who design freely available user-centred technologies which

- regardless of their financial usability - create the foundations of (digital) coexistence and social added value". From 2016 to 2024, approximately 25 innovative projects will be funded in each of 16 funding rounds. Self-employed programmers and small teams living in Germany can receive a maximum of 47,500 euros for each project. The results must be made publicly available under an open source licence.

Industry representatives criticise the strong **focus on innovation at the** NLnet Foundation and most funding programmes. Funding is given either to completely new developments - such as through the Prototype Fund - or at least to the development of new functions for existing open source software. Often, however, it is not enough to have and implement individual innovative ideas. Projects also have to have the usual range of market functions in order to be competitive. One project was rejected by the Prototype Fund, probably because a similar function was already available in a centralised system and it was apparently not considered a significant innovation for users to port it to a decentralised system.

In addition, a non-negligible part of the work on open source projects goes into **the maintenance of software and any necessary infrastructure** (server, etc.). The purely technical operation of this infrastructure (e.g. server costs etc.) is almost never funded. Thus, new functions are always developed for software, which, including the infrastructure, is no longer checked for errors. This also applies to common software that is already used by many people. Is this open source software a "library" that can be used by many others?

---

[311] See *Open Knowledge Foundation, available at:* https://okfn.de/ or see *Wikipedia*, available at: https://de.wikipedia.org/wiki/Open_Knowledge_Foundation_Deutschland. The Open Knowledge Foundation Deutschland e. V. (OKFDE) is a non-profit organisation based in Berlin that was founded in 2011. It engages in several projects, including in the areas of Freedom of Information, Open Government, Open Data, Civic and Public Interest - Tech as well as
Education for the dissemination and use of "open knowledge". The organisation is part of the international Open Knowledge Network from a total of 24 countries. The association's work is independent, non-partisan, interdisciplinary and non-commercial.

projects - is also used by proprietary systems, the problem of poorer maintenance is becoming more and more important, which was illustrated by one of the interviewees with the following comic[312] (see Figure 17).

The lack of support for the **maintenance, upkeep and care of** important and widely used open source software has also been a decisive reason for some major **security breaches in** recent years.[313]

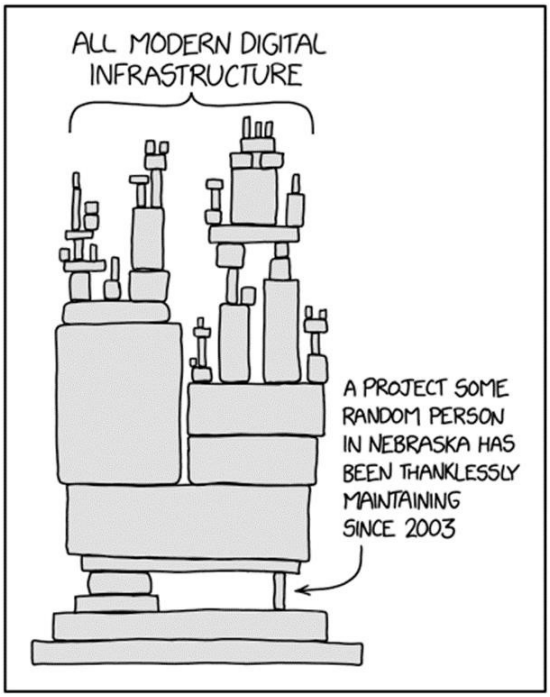


Figure 17: Consequences of lack of maintenance for open source software

One service explains that they are now trying to ensure the maintenance of their own infrastructure through donations. However, the success of such a campaign cannot really be planned. The XSF states,

[312] Source: Investigations.

[313] Examples include the "Log4Shell" vulnerability in the Java programming language or the bug in the open source library OpenSSL "Heartbleed", which has since been fixed and affected the TLS protocol. See on "Log4Shell" *BSI*, press release of 16.12.21, Update: Warning level red: vulnerability Log4Shell leads to extremely critical threat situation, available at: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4 Shell_WarnstufeRot.html as well as on "Heartbleed", see Frankfurter Allgemeine Zeitung, "Heartbleed" is not yet stopped, available at: https://www.faz.net/aktuell/wirtschaft/netzwirtschaft/bsi-warnt- heartbleed-ist-noch-nicht-gestoppt-12898921.html.

Even with small amounts of funding, maintenance, upkeep and care could be carried out sustainably. Finally, the **bureaucracy and time** required in many areas, which are lamented with a

The fact that the application process is not easy is also seen as an obstacle to the funding of open source projects. In particular, there is no easily accessible information about funding opportunities, which requires a lot of time to find. Also in the case of funding for open source, the time span from the application for funds to the payment is quite long and the approval is naturally uncertain. For this reason, only larger projects are applied for at all; smaller projects have long been implemented by the time the funds are paid out.

In the public sector, the Bundeskartellamt has come across examples of the **use of open source**, albeit initially less concretely in the area of messenger and video services. Examples include the open source strategy of the state of Schleswig-Holstein[314] , the open source strategy "LiMux" of the city of Munich[315] and the initiative of the city of Dortmund[316] **.** Referred to

[314] In the coalition agreement of the black-green-yellow state government concluded in 2017, Schleswig-Holstein had stated that all civil servants and employees of the state, including teachers, would be equipped with open source software. The responsible digital minister Jan Philipp Albrecht (Bündnis 90/Die Grünen) has - according to press reports - now concretised the plans. By the end of 2026, Microsoft Office is to be replaced by Libre Office and later Windows by Linux. Cf. *Heise*, available at: https://www.heise.de/news/Schleswig-Holsteins-Digitalminister-Albrecht-ueber-den-Wechsel-zu- Open-Source-6221361.html and *LinuxNews*, available at: https://linuxnews.de/2021/11/schleswig- holstein-macht-ernst-mit-open-source/.

[315] In Munich, an open source strategy had been pursued that had become known under the catchword "LiMux". After difficulties, the project was discontinued in 2017. In the meantime, however, there are plans to continue the open source strategy again. See *Wikipedia*, available at: https://de.wikipedia.org/wiki/LiMux, *Deutschlandfunk Nova*, available at: https://www.deutschlandfunknova.de/beitrag/linux-versus-microsoft-m%C3%BCnchen-will-wieder-zurueck-zu-mehr-open-source.

[316] Another positive example is the city of Dortmund, which wants to prioritise the use of open source software over proprietary software in the future and has set this out in a "Memorandum on Digitalisation 2020 to 2025". Cf. *Der Neue Kämmerer*, available at: https://www.derneuekaemmerer.de/digitalisierung/news/dortmund-setzt-auf-open-source-software-13460/, *Do-Foss*, available at: https://blog.do-foss.de/beitrag/freie-software-ist-von-jetzt-an- standard-in-dortmund/, *Golem*, available at: https://www.golem.de/news/verwaltung-dortmund- beschliesst-open-source-fuer-die-stadtverwaltung-2104-155449.html.

will also be looking at the Corona warning app for the time after the source code has been published. More than 65,000 volunteer software experts had looked at the already published source codes and made their own suggestions for improvements.[317] A switch to open source software in the administration is also being discussed abroad, for example in Switzerland[318] , in the city of Barcelona[319] or in the city of Tirana, which has already decided to use open source software in 2018. [320]
Especially with regard to **messenger and video services,** some universities use free messenger systems, such as the Matrix protocol.[321] These include, for example, the University of Augsburg[322] , the

[317] See *Die Bundesregierung*, available at: https://www.bundesregierung.de/breg-de/suche/corona- warn-app-1757082, *ZEIT ONLINE*, available at: https://www.zeit.de/digital/2020-05/corona-app- open-source-projekt-programmcode-quellcode and *Science Media Center*, available at: https://www.sciencemediacenter.de/alle-angebote/fact-sheet/details/news/wie-apps-und- programmcode-ueberprueft-werden/.

[318] In Switzerland, a new guide from the Swiss Confederation provides recommendations and background knowledge on the use and dissemination of open source software (OSS) in the federal administration to support its use. See *Guide of the Swiss Confederation,* available at: https://www.pro-linux.de/news/1/27770/schweiz-neuer-leitfaden-unterst%C3%BCtzt-einsatz- von-oss-in-der-verwaltung.html.

[319] The City of Barcelona no longer uses Microsoft software - e.g. the e-mail client Outlook - in its administration, even though Windows will be retained as the operating system for the time being. The switch to Linux has been planned. See also *El Pais*, available at: https://elpais.com/ccaa/2017/12/01/catalunya/ 1512145439_132556.html. See *Heise*, available at: https://www.heise.de/newsticker/meldung/Stadt-Barcelona-setzt-auf-Open-Source-und-Linux-3944797.html.

[320] Cf. LibreOffice, available at: https://blog.documentfoundation.org/blog/2018/11/22/municipality- of-tirana/.

[321] Within the framework of the sector enquiry, it was not possible to verify how the universities implement the matrix protocol with regard to the protective handling of university staff and students' data.

[322] Cf. *University of Augsburg*, available at: https://www.uni-augsburg.de/de/fakultaet/mntf/physics/facilities/itservices/elequick/.

University of Bielefeld[323] , the Ruhr University of Bochum[324] , the Technical University of Chemnitz[325] , the Technical University of Dresden[326] , the University of Heidelberg[327] , the University of Innsbruck[328] , the Leibniz University of Hanover[329] or the University of Osnabrück[330] . The open source strategy of the state of Schleswig-Holstein should also be mentioned here, in the context of which a free messenger client is to be used in public administration.[331]

The expectations of the surveyed services towards the public sector formulated in the investigations did not refer solely to a review of funding practices and deployment opportunities for open source, but in general to the **use of data protection-friendly services**. This is linked to the hope of increasing the chances of less well-known data protection-friendly services in other areas as well.

The Bundeskartellamt's findings from the investigations and its own research suggest that the public sector can expand its use of privacy-friendly messenger and video services. Industry representatives and stakeholders of free messenger systems have provided numerous examples that considerable effort and persuasion is needed to get privacy-friendly messenger and video services that are **less well-known than incumbent services to be** considered. Competitors of incumbent services have referred to **tender conditions,**

---

[323] See *Bielefeld University*, available at: https://uni-bielefeld.de/einrichtungen/bits/services/communication/teamchat/howto/element-android/.

[324] Cf. *Ruhr University Bochum*, available at: https://www.it-services.ruhr-uni-bochum.de/services/issi/element.html.de.

[325] Cf. *Chemnitz University of Technology*, available at: https://www.tu-chemnitz.de/urz/groupware/chat/doku/nutzen.html.

[326] Cf. *Ruhr University Bochum*, available at: https://www.it-services.ruhr-uni-bochum.de/services/issi/element.html.de.

[327] Cf. *University of Heidelberg, available* at: https://www.urz.uni-heidelberg.de/de/service-katalog/collaboration-und-digitale-lehre/heichat.

[328] Cf. *University of Innsbruck*, available at: https://www.borncity.com/blog/2021/05/03/uni-innsbruck-setzt-auf-matrix-element-statt-auf-ms-teams/.

[329] Cf. *University of Hanover*, available at: https://www.luis.uni-hannover.de/de/services/kommunikation/matrix-messenger/.

[330] Cf. *University of Osnabrück*, available at: https://www.wiwi.uni-osnabrueck.de/fachbereich/edv_betreuung/anleitungen_hinweise/element_chat_ehemals_riot.html.

[331] See *Golem*, available at: https://www.golem.de/news/messenger-schleswig-holstein-will-matrix- chat-fuer-verwaltung-2007-149687.html.

which tend to reduce the chances of data protection-friendly services. This practice could be reviewed and consideration given to whether more data protection-friendly alternatives exist compared to the application chosen so far and could at least be used additionally in the public sector.

Public radio and television in particular could have a **multiplier effect.** The opportunity to encourage as many different consumer groups as possible to use privacy-friendly messenger systems, at least by offering them as a communication channel, has so far often remained unused - even in the case of well-known programmes and channels.

- unused. [332]

[332] Examples are the television programmes "ARD-Morgenmagazin", see *ARD*, available at: https://www.daserste.de/information/politik-weltgeschehen/morgenmagazin/specials/moma-bei-whatsapp-100.html; "Live nach Neun", see *ARD*, available at: https://www.daserste.de/information/politik-weltgeschehen/morgenmagazin/specials/moma-bei-whatsapp-100.html; the radio programme Kontrovers, see *ARD,* available at: https://www.daserste.de/information/ratgeber-service/live- nach-neun/whatsapp-102.html, the radio stations*; Bremen Eins*, available at: https://www.bremen eins.de/kontakt/kontakt-startseite-116.html; *Bremen Zwei*, available at: https://www.bremen zwei.de/kontakt/kontakt-startseite-114.html; *Bremen Vier*, available at: https://www.bremen vier.de/kontakt/kontakt-startseite-100.html; *Bremen Next,* available at: https://www.bremen next.de/kontakt/kontakt-136.html; COSMO, see *WDR,* available at: https://www1.wdr.de/ radio/cosmo/ueber-uns/kontakt/index.html; 1Live, see *WDR, available at*: https://www1.wdr. de/radio/1live/on-air/kontakt/whatsapp260.html; *hr3*, available at: https://www.hr3.de/service/hr3- per-whatsapp-erreichen-0800--33-33-307,whatsapp-112.html; rbb 88.8, available at: https://www.rbb888.de/; *WDR 2, available* at: https://www1.wdr.de/radio/wdr2/kontakt/index.html; *SR 1*, available at: https://www.sr.de/sr/sr1/wir/sr1_social_media100.html; *SR 3*, available at: https://www.sr. de/sr/sr3/service/sr3_social_media100.html; *UNSERDING*, available at: https://www.unserding.de/unserding/unserding_at_whatsapp_100.html; *SWR 4 Rheinland Pfalz*, available at: https://www.swr.de/swr4/kontakt/kontakt-per-whatsapp-100.html; *MDR*, available at: https://www.mdr.de/sachsenradio/whats-app-sprachnachricht-sachsenradio-100.html; the morning programme of *MDR* Sachsen-Anhalt, available at: https://www.mdr.de/mdr-sachsen- anhalt/mdr-sachsen-anhalt-bei-whatsapp100.html as well as the team of the podcast "Ab 21" of *Deutschlandfunk Nova*, available at: https://www.deutschlandfunknova.de/podcasts/download/ab- 21 on WhatsApp. In addition, the radio station 1Live uses *Snapchat*, available at: https://www.snapchat.com/add/wdr1live. *Bayern 2, for example, can be reached via* WhatsApp and Telegram at: https://www.br.de/radio/bayern2/service/newsletter/bayern-2-newsletter-whatsapp-telegram100.html; *SWR 1 Baden-Württemberg*, available at: https://www.swr.de/swr1/bw/artikel-.

In the case of **cities and municipalities,** random samples have also shown that the most widespread messenger systems are used here.[333]

In the area of the federal administration, too, there are opportunities to promote communication via data protection-friendly and legally compliant messenger systems, as the research has shown. It must be taken into account that public bodies must also be able to reach their addressees.

In the **education sector,** the situation is more difficult to assess and oversee. For the **school's communication with teachers, parents and pupils,** there are handouts from the

swr1-auf-whatsapp-100.html; *SWR 1 Rheinland Pfalz*, available at: https://www.swr.de/swr1/rp/kontakt/article-swr-8188.html and *SWR 4 Baden-Württemberg*, available at: https://www.swr.de/swr4/kontakt/index.html. WDR offers to send users news from and for NRW via Facebook Messenger or Telegram. In addition, Facebook Messenger also gives users the opportunity to ask for topics themselves or - as with Siri and Alexa - to have a little chat with the WDR aktuell Bot. Cf. *WDR*, available at: https://www1.wdr.de/nachrichten/handy-nachrichten-wdr-aktuell-100~_redirectedFromOffline- true.html. The "tagesschau" offers to send the most important news twice a day and also breaking news via Messenger. This possibility is opened for the messengers of Apple, Facebook, Telegram and Notify. It is not possible to send news via WhatsApp because WhatsApp no longer tolerates newsletters since the end of 2019, cf. *tagesschau*, available at: https*://www.tagesschau.de/inland/messenger-113.html.*

[333] Random checks have shown, for example, that Bonn Information is also available via WhatsApp for questions and concerns. A ticket for a city tour or for guided city tours can also be reserved via this app, see *City of Bonn*, available at: https://www.bonn.de/bonn- erleben/anreisen/service-whats-app.php. The city of Nuremberg informs its citizens via Telegram and Notify about important news from the Nuremberg city area and the city administration. The registered citizens receive the update for Nuremberg once a day from Monday to Friday. In addition, the city also informs its citizens about important events with a message, see *City of Nuremberg*, available at: https://www.nuernberg.de/internet/stadtportal/messenger_anmeldung.html**.** The city of Reutlingen offers Corona messages via Telegram and Notify. Municipalities as well as the associated municipal institutions (e.g. municipal utilities, municipal electricity or daycare centres) offer citizen services via WhatsApp, see e.g. Municipality of *Wadgassen,* available at: https://www.wadgassen.de/rathaus-service/buergerservice/whatsapp/ or *Municipality of Vettweiß*, available at: https://www.vettweiss.de/news/news-archiv/whatsweiss.php.

Conference of Ministers of Education and Cultural Affairs and various school ministries of the Länder.[334] This is mainly due to the Corona pandemic and the requirements of home schooling. The measures are very different. However, many schools deviate from them and go their own ways, possibly because the solutions offered do not meet the practical requirements.

Whether and how consumers could be encouraged to use messenger and video services that are not **only practicable but also privacy-friendly at the same time is** discussed in the following chapter.

2. Activation of the demand side

As the results of the investigation have shown, all messenger and video services see further consumer education as an essential element of a data protection strategy. The Bundeskartellamt shares this view. Provided that initiatives to this end were reoriented and intensified, data protection-friendly services could possibly have better chances of prevailing over competitors. Therefore, in the following, the information deficits that exist among consumers will first be examined in more detail (see a) and b)). Subsequently, consequences for consumer policy are discussed, which should be oriented towards the situation of consumers (see c)).

a) Data protection as a quality feature?

Consumer preferences - in terms of privacy - are context-specific, inconsistent and not always well-considered (on the so-called privacy paradox, see also under F.II.2).[335] When consumers choose a messenger and video service, it is a composite transaction.[336] Their main focus is on the product "messaging and video conferencing", whereas the data processing transaction as a

---

[334] Cf. e.g. E.g. *Kultusministerkonferenz*, available at: https://www.kmk.org/themen/bildung-in-der-digital-welt/distanzlernen.html and *Land Brandenburg*, available at: https://bildungsserver.berlin-brandenburg.de/online-lernen-tools.

[335] See *Kerber*, Digital markets, data and privacy: Competition Law, Consumer Law and Data Protection, Joint Discussion Paper Series in Economics No. 14, 2016, p. 7, available at: https://www.uni-marburg.de/fb02/makro/research/magkspapers/paper_2016/14-2016_kerber.pdf.

[336] See *Jentzsch*, State-of-the-Art of the Economics of Cyber-Security and Privacy, IPACSO - Innovation Framework for ICT Security Deliverable, 2016, p. 35, available at: https://www.econstor.eu/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf.

time-lagged effect receives less attention. This also applies to free offers, where payment may be made via the data processing transaction or other functions.

Messenger and video services will only invest in data protection to the desired extent and communicate or even advertise this in a comprehensible way if consumers consider data economy, data protection compliance and data security as a quality feature of a service. Data protection could then become a **competitive advantage of** services. So far, this only applies to some services that advertise with many data security and data protection measures, thus using data protection as a comparative competitive advantage and charging a corresponding fee for it.

In order for data-protecting and data-protecting activities of the services to increase across the board, consumers must not only be informed, but also motivated to demand the necessary information from the services by only using the clients of those messenger and video services that enable **informed decisions.**

However, it is not only necessary to activate consumers and awaken in them the need to use data-protecting services. They also have to find out with reasonable effort about the data protection quality of the desired product "messenger and video service".

inform themselves and make comparisons. Currently, this is only possible to a very limited extent, e.g. via websites of IT experts or comparative presentations of certain institutions. However, the features checked here are mostly based on the range of tasks and the core competences of the publishing institution. Moreover, the information quickly becomes outdated, if it is searched for and found by consumers at all. The data protection quality of a service is thus difficult to determine.

Whether and to what extent consumers are able to evaluate the quality characteristics of a product can be illustrated with the so-called **quality uncertainty approach**[337] . Three categories of goods are formed, which differ according to whether the quality of a product can be observed before and/or after purchase. In the case of so-called **search goods,** consumers know the quality of the product before and after purchase. In the case of so-called **experience goods, the** quality of the product can only be assessed after the purchase. So-called

---

[337] See *Nelson*, Advertising as Information, in: Journal of Political Economy 1974, 729, available at: https://www.jstor.org/stable/1837143?seq=1, and *Darby/Karni*, Free Competition and the Optimal Amount of Fraud, in: Journal of Law and Economics 1973, 67, available at: https://www.journals.uchicago.edu/doi/10.1086/466756.

Confidence goods are characterised by the fact that the quality of the product remains hidden from consumers even after the purchase.

When it comes to data protection quality, some consumers are currently likely to describe it as an **experiential good.** As the sector enquiry has shown, consumers can hardly get an overview of all data protection-relevant features of the favoured product before buying. The data protection practices and information behaviour of the services are inconsistent and non-transparent. For example, users may only find out when they use a service that they have to disclose personal data, e.g. also for setting up an account in order to be able to use certain functions beyond the basic ones. Most consumers would probably speak of a **trusted good.** Certain groups of consumers have so far ignored any data protection aspects in their decisions, whether out of ignorance, disinterest, lack of time or simply because they have given up in the face of the complexity of obtaining information (see also F.II.2.). In addition, even interested and informed users are usually not aware of the extent to which their data is collected and by whom and for what purpose it is used.

Finally, the actual flow of data can only be verified with considerable technical effort and often not at all with regard to the concretely transmitted content. Under such conditions, no informed decisions can be made. The subject matter is too complex for consumers to be able to improve their level of information simply by lowering the **search costs**[338] . Rather, the information must be prepared in such a way that its relevance is understood, it is comprehensible or can be understood in a reasonable amount of time.

[338] Search costs should be interpreted broadly here to include the costs of any alternative valued use of resources that must be expended to conduct information searches.

b) Less information gap - more demand for data protection?

In information economics approaches[339] it is - beyond the above mentioned quality uncertainty approach - first of all about reducing **quality uncertainty. Consumers** can be uncertain about the **(data protection) quality of** the chosen service before and after "concluding the contract". Two types of activities are suitable for reducing information disadvantages. So-called. **Screening activities** can be undertaken both outside and inside a contractual relationship. Screening can include all conceivable search activities. It includes everyday search activities on the internet or research in other media as well as more complex regulatory systems, such as self-selection schemes. Here, a certain contractual condition leads to the fact that only the person who fulfils this condition concludes the contract (cf. excess clause in insurance policies).[340] **Information transmission** activities **("signalling")** can also be suitable for reducing information disadvantages. Signalling is possible both for fixed, unchangeable properties (so-called indices) and for properties that are observable but can still be changed by the informant (signals in the narrow sense).[341] The latter category probably includes data protection quality, which could be signalled by services to consumers via a wide variety of measures.
However, problems of asymmetric information distribution cannot be blamed solely on deficits of the market mechanism. Critics

[339] Cf. the fundamental work of *Stigler*, The Economics of Information, in: The Journal of Political Economy 1961, 213, available at: https://home.uchicago.edu/~vlima/courses/econ200/ spring01/stigler.pdf and *McCall*, The Economics of Information and Job Search, in: Quarterly Journal of Economics, 1970, pp. 113 - 126. Information economic approaches are part of the New Institutional Economics. This comprises various theoretical explanatory approaches, which are essentially divided into four schools: The property rights approach or theory of rights of disposal, the transaction costs approach, the principal-agent approach and information economics approaches, cf. e.g. Picot, The New Institutional Economics. *Picot*, Ökonomische Theorien der Organisation - ein Überblick über neuere Ansätze und deren betriebswirtschaftliches Anwendungspotential, in: *Ordelheide/Rudolph/Büsselmann* [eds]: Betriebswirtschaftslehre und Ökonomische Theorie, 1991,
S. 143.

[340] Cf. *Woratschek*, Betriebsform, Markt und Strategie, 1992, p. 96.

[341] Cf. *Spence*, Informational Aspects of Market Structure: An Introduction, in Quarterly Journal of Economics 1976, 591, 593. The efficiency of information measures can be judged by the costs of signalling and screening activities.

The explanatory approaches of information economics point to other important factors that can also have an impact on consumer behaviour and the efficiency of market outcomes. These can be, for example, transaction costs, which as costs of initiating and executing contracts exceed information costs. However, measures that improve consumers' level of information must above all be able to capture their individual characteristics and perceptions - as described by the Privacy Paradox. Recent behavioural economic explanations[342] can serve as a theoretical background, but also the New Institutional Economics[343] , which has been used in various research areas to analyse exchange relationships and their risks and to design them in a risk-minimising and cost-efficient way. Among other things, behavioural economics has to thank considerations according to which information cannot be perceived and processed in any quantity and in any short time. A too large, confusing offer of decision alternatives will tend to lead to decisions being refused or postponed.[344]

More than behavioural economic approaches, neoinstitutional economic explanatory theories offer generalisable, easily understandable and clearly structured recommendations on how information asymmetries can be overcome. They are also suitable for analysing the exchange relationship between companies and consumers in matters of

---

[342] The concept of "bounded rationality" is essential. Cf. *Simon,* Rational Choice and the Structure of Environments, in: Psychological Review 1956, 123, available at: https://pdfs.semanticscholar.org/23a9/4ce42fe0d50f5c993f34d4c9602f8aeac507.pdf. Behavioural economic explanations are based on empirical and experimental observations as well as game-theoretical experiments.

[343] See for an overview e.g. *Terberger*, Neo-institutionalist Approaches, 1994, and *Richter/Furubotn*, New Institutional Economics, 1996. New Institutional Economics comprises various theoretical explanatory approaches, which are essentially divided into four schools: The property rights approach or theory of rights of disposal, the transaction cost approach, the principal-agent approach and information economics approaches, cf. *Picot*, Ökonomische Theorien der Organisation - ein Überblick über neuere Ansätze und deren betriebswirtschaftliches Anwendungspotential, in: *Ordelheide/Rudolph/Büsselmann* [eds:] Betriebswirtschaftslehre und Ökonomische Theorie, 1991,
p. 143, as well as *Kaas*, Marketing and New Institutional Economics, in: *Kaas* [ed:] Contracts, Business Relationships, Networks - Marketing and New Institutional Economics, 1995, p. 1. Even though the different approaches focus on different aspects of a transactional relationship, they are based on common basic assumptions about the motivation of economic agents.

[344] Gladly summarised as a policy change from "A lot helps a lot!" to "Keep it simple!".

Data protection as a product property. The **assumptions about human behaviour**[345] are reminiscent of current trends in research on the **consumer model**. Recently, a more differentiated consumer model with responsible, vulnerable or trusting consumers[346] has been discussed.[347] In the meantime, there seems to be a broad consensus that differences between consumers in terms of their perception, emotion and motivation must be taken into account.[348] The starting point of the neoinstitutional economic analysis is precisely the individual behaviour of consumers.

---

[345] In the neoinstitutional economic model, the human image of the rationally controlled homo economicus, which is the basis of classical microeconomic explanations, is abandoned. Instead, behavioural determinants of a psychological and sociological nature as well as cultural and personality-related influences are included, cf. e.g. Richter/Furubotn, Neue Institutionenökonomische Modelle. *Richter/Furubotn*, Neue Institutionenökonomik, 1996, or *Aufderheide/Backhaus*, Institutionenökonomische Fundierung des Marketing: Der Geschäftstypenansatz, in *Kaas* [ed.]: Contracts, Business Relations, Networks, 1995, p. 43.

[346] European case law has so far been based on the average consumer who is of sound mind or reasonably well informed and reasonably observant and circumspect, cf. ECJ, Judgment of 16.07.1998, C- 210/96, [1998] ECR I-4657, para. 31 - *Gut Springenheide*. German case law has confirmed this
and finally further specified with "situation-adequate attention", cf. for example
BGH, judgement of 20.10.1999, ref. I ZR 167/97, juris marginal no. 20 - *Oriental carpet design*.

[347] Cf. *Micklitz*, Der vertrauende, der verletzliche oder der verantwortungsvolle Verbraucher? Plädoyer für eine differenzierte Strategie in der Verbraucherpolitik, Stellungnahme des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim BMELV, 2010, available at: https://www.vzbv.de/sites/default/files/downloads/Strategie_verbraucherpolitik_Wiss_Beirat_BMELV_2010.pdf and *Pagel***,** Das Verbraucherleitbild in der digitalen Welt, Impulsvortrag, o. Jg., Hochschule Mainz**,** available at: https://mffjiv.rlp.de/fileadmin/MFFJIV/Verbraucherschutz/Digital-Dialog_Impulsvortrag_210317_SP.pdf and *Ernste*, Verbraucherschutz und Verhaltens-ökonomik. Zur Psychologie von Verhalten und Kontrolle, IW Analysen 106, 2016, available at: https://www.iwkoeln.de/studien/iw-analysen/beitrag/dominik-enste-mara-ewers-christina-heldman-regina-schneider-verbraucherschutz-und-verhaltensoekonomik-291323.html.

[348] Cf. *Becker*, Bundeskartellamt und Verbraucherschutz, ZWeR, 2018, 229, 244; also BDI, Study Verbraucherleitbild und Positionsbestimmung zum mündigen Verbraucher, 2014, available at: https://bdi.eu/media/publikationen/?publicationtype=Studien#.

economic subjects in the face of uncertainty.[349] The other assumptions also correspond in their basic features to typical observable behaviour patterns of users in their dealings with messenger and video services: utility maximisation is sought, but only limited rational action is taken. Consumers' capacities to absorb information are limited and (data protection) risks are not assessed uniformly. Finally, it is assumed that economic agents - i.e. all market participants, including consumers and services - always follow their self-interest, even if this is at the expense of their contractual partners.[350] Against this background, different manifestations of **information asymmetries are** analysed, which consumers have to deal with when deciding on one or more messenger and video services. Information economics approaches propose basic mechanisms to mitigate information disadvantages and reduce risks.
In addition to quality uncertainty, **two other manifestations of information asymmetries in** data protection issues are relevant for consumers when they conclude contracts with services. An asymmetric distribution of information can be the origin of conflicts if the better-informed contractual partner exploits its information advantage in its own favour after concluding the contract.[351] Thus, consumers cannot judge or assess the **fairness of the service after entering into a contractual relationship** before and after conclusion of the contract. For the analysis, a distinction is made between the contracting party, who as the "headmaster" assigns tasks and has better information about the cooperation goal and does not want to be harmed, and the "agent", who has better information about the object and task.[352] Transferred to a

---

[349] Methodological individualism is assumed. Cf. *Richter*, Sichtweise und Fragestellungen der Neuen Institutionenökonomik, in: Zeitschrift für Wirtschafts- und Sozialwissenschaften, 1990, 571, 573.

[350] Cf. *Williamson*, The Economic Institutions of Capitalism, 1990, p. 54.

[351] Opportunistic behaviour is also addressed in a relevant BDI study, see *BDI*, Verbraucherleitbild und Positionbestimmung zum "Mündigen Verbraucher", 2014, p. 14, available at: https://bdi.eu/media/presse/publikationen/gesellschaft-verantwortung-und-verbraucher/BDI_Studie_zum_muendigem_Verbraucher.pdf.

[352] These considerations are the basis of the so-called principal-agent approach, which originally refers to contractual relationships on the same side of the market, but can also be used for the analysis of other contractual relationships. Cf. for an overview of the principal-agent approach e.g. *Richter/Furubotn*, Neue Institutionenökonomik, 1996. *Matten* has used the principal-agent approach to examine the relationship between companies and stakeholders, cf. *Matten*, Management ökologischer Unternehmensrisiken, 1998, p. 198.

contract between providers and consumers, consumers would play the role of headmaster, while the providers of messaging and videoconferencing functions would act as agents. If, for example, a service violates the privacy rights of users after the contract has been concluded, and the users subsequently become aware of this, the service had **hidden intentions** (so-called *hidden intention* or *hold-up*). The consumer misses out on benefits if his or her investment in the use of the service becomes worthless or loses value due to the infringement.

In the case of **hidden actions** (so-called *hidden action* with *moral hazard*), the violation of data protection rights by the service provider (agent) remains completely unknown to the consumer (principal) or only becomes apparent after some time. *Moral hazard* could also be spoken of if, for example, services would collect and use more consumer data than is stated in the privacy policy of the service and the consumer does not discover this at all or discovers it much too late. Consumers might shy away from concluding contracts because of these risks. Agents (here: messenger and video services) can counter this through targeted **risk communication.** In principle, all measures that increase the authority of consumers as headmasters and alleviate the fear of opportunistic behaviour can be communicated.[353]

Provided that measures are taken to reduce consumers' information disadvantages, they could be encouraged to be more proactive. Privacy-friendly services would then have a better chance of being noticed and selected. However, this will only succeed if consumers' awareness of the protection of their data can be raised. The data protection quality of messenger and video services must emerge from their shadowy existence and become visible. Further measures must be taken to support this.

c) Consequences for consumer policy

To put it simply, measures to protect consumers are always justified from the perspective of information economics if they are exposed to existing information asymmetries. This does not necessarily have to be reflected in state measures.

---

[353] For a practical application of the explanatory approaches to risk communication, see *Matten,* Management ökologischer Unternehmensrisiken, 1998, p. 203. In the case of moral hazard in individual economic contractual relationships on the same side of the market, incentive and reward systems can also be used to reduce risk.

lead to a market solution. On the contrary, market-based solutions are considered quite suitable for solving the problems of adverse selection and moral hazard. In principle, the Bundeskartellamt also prefers market-based solutions in order to close legal enforcement deficits or gaps in consumer protection and to help data protection achieve a broader impact. This includes, first of all, instruments that reduce the costs of information searches and improve the level of information of consumers.[354] The extent to which it is possible to advance **data protection quality as a competitive parameter** depends largely on the subjective perception of consumers. Ultimately, it is this perception that determines the type and extent of information intake and the information-seeking activities.[355]

As shown above, however, the problems of asymmetric information distribution are apparently not solely responsible for the fact that consumers have so far only perceived data protection as a competitive parameter to a very limited extent. If consumers have **no particular interest in the** quality of a product or service being improved, more information or information that is easier to find will not trigger any behavioural changes and the market outcome will not improve. Market-related measures, such as the introduction of information obligations or quality labels, then do not lead to success. As far as **data protection as a quality characteristic is concerned, it is** not apparent so far that many consumers base their choice of messenger and video service on data protection friendliness. If they do try, they have to cope with very unevenly distributed information - in favour of the services, to their detriment. In a technically based

[354] Cf. *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik - Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, available at: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering. From a scientific (especially information economic) point of view, these could be, for example, information obligations for providers, the lifting of information restrictions, the definition of standards or the prohibition of misleading information. Licensing restrictions and similar measures are viewed more critically than information obligations. This is not the case if information obligations are useless because their addressees are not interested in the information or additional information cannot compensate for the information asymmetries, as is the case with goods of trust - here data protection. See e.g. *Sinn*, Verbraucherschutz als Staatsaufgabe, in: Perspektiven der Wirtschaftspolitik, 2003, Jg.4, pp. 281 - 294, available at: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2516.t01-2-00009m. If these measures are not sufficient, a separate state information service may be justified.

[355] Cf. *Matten*, Management ökologischer Unternehmensrisiken, 1998, p. 203.

It is even more complicated in the second sector: consumers would first have to find out what information is relevant at all, then search for it, gain a basic understanding and finally form an overall judgement from several criteria and compare them.
As a result, messenger and video services, as providers of messaging and video conferencing services, feel **little pressure to** give higher priority to better information on the data protection practices of their service and to strive to enable consumers to make informed choices. In the course of current developments, further challenges arise: the interoperability rules in the DMA will pose further challenges to data security and thus data protection. The services are technically set up differently. Many well-known services have been designed as closed systems. The data of all parties involved may thus be exposed to new risks when interoperability is introduced.
At the same time, the information situation can become even more opaque for consumers. Therefore, in the Bundeskartellamt's current view, purely market-based measures may not be sufficient to establish data protection as a competition parameter. State intervention may then be an option that needs to be examined. The Bundeskartellamt takes up the proposal of an industry representative who suggested a **rating** under state responsibility not only to reduce the unequal distribution of information, but also to activate both messenger and video services as well as users in matters of data protection. However, the problems of asymmetric information distribution can shift to the relationship between **consumers and the intermediary** when information intermediaries such as rating agencies are used. Also, the extent to which the rating grade is an actual quality judgement can hardly be assessed directly by the consumers. The rating must be designed in such a way that these new information problems are minimised and the goal of advancing data protection as a competitive parameter is implemented in the best possible way.

III. Evaluate data protection quality comparatively and transparently

In the following, the background and concept of rating are first introduced and the basic requirements for a transfer to the data protection area are presented (see 1.). Then it will be examined to what extent there are connecting factors for such an information instrument in consumer law and policy (see **Error! Reference source could not be found.**). Finally, advantages and disadvantages are outlined from an institutional economics perspective (see 3.). Against this background, concrete considerations for a data protection rating are formulated and related to the findings from the investigations (see 4.).

1. Background and main characteristics

The term "rating" is known in particular from the credit industry. There it is an assessment of the economic situation and the creditworthiness of companies, institutions or states. Companies that participate in a rating procedure are assigned to a credit rating level or rating class on the basis of an ordinal scale.

An essential part of the rating procedure is the so-called **scoring model**. In general terms, statistical methods are used to determine the probability of occurrence of certain (loss) events with the aim of minimising the risks arising from existing information asymmetries. The score values - which are converted into rating grades or classes - are calculated according to **qualitative and quantitative assessment criteria.** For a credit rating, for example, liquidity, capital structure, etc. are examined on the one hand, and on the other hand, external influencing factors resulting from special features of the industry or the country risk.

These assessment criteria are assigned point values, weighted and summed up. The result is an assessment of the probability of default, which is usually presented and published with a sequence of letters and/or numbers.[356]

Scoring models are not only used by companies, for example to evaluate customers, sales territories or products. Online retailers and banks or insurance companies also assess the creditworthiness of their customers. They often receive the score values for their (potential) customers from specialised companies, the so-called credit agencies.

At the same time, however, they sometimes also create their own score values based on customers' previous transactions and pass on their data to other companies.[357]

---

[356] Cf. e.g. E.g. *Wikipedia*, available at: https://de.wikipedia.org/wiki/Rating; *Finanzen.net*, available at: https://www.finanzen.net/wirtschaftslexikon/rating, *SpringerGabler*, available at: https://www.gabler-banklexikon.de/definition/rating-60805, *Bundeszentralle für politische Bildung,* available at: https://www.bpb.de/kurz-knapp/lexika/lexikon-der-wirtschaft/20479/rating/.

[357] This topic is the subject of the sector enquiry "Scoring in Online Shopping", which the *Bundeskartellamt* initiated in March 2022, cf. https://www.bundeskartellamt.de/SharedDocs/Publication/DE/Press Releases/2022/31_03_2022_SU_Scoring.pdf? blob=publicationFile&v=5. The study examines whether online retailers adhere to the data and consumer protection legal framework when conducting credit checks. For example, the question of whether and how online traders obtain permission to carry out creditworthiness checks from the ordering party will be investigated.

Rating procedures for credit risk are also carried out both by banks for internal bank credit assessments and by independent rating agencies. The best-known private rating agencies for the credit industry are Standard and Poor's[358] , Moody's[359] and Fitch[360] . The rating agencies do not make any investment recommendations with the ratings, but only provide an assessment of the default risk. Beyond the underlying scoring model, a rating is characterised by the following **essential features**. First, a goal must be formulated. Transferred to the area of data protection, this would be **exclusively the assessment of the data protection risk**[361] of a messenger and video service.
Other criteria, such as accessibility based on the user base or new functions in terms of user experience, are left out. Furthermore, a **rating authority** is necessary that is responsible for the procedure and publishes the results. In principle, this can be a private company or an authority. However, a certain degree of recognition and a **reputation that** promises trustworthiness and competence is necessary to achieve the necessary acceptance among market participants. The body should also be independent in the sense that it is not mixed up with other tasks in the sector.
As just described, the compilation of **criteria** that form the score value including, if applicable, a weighting and designation (e.g. AAA in the credit sector), class formation of the scale and ranking is the essential core of the rating. The rating must then be **published. A regular and, if necessary, occasion-related re-evaluation** must take place, since the speed of development of the industry is high and corresponding changes in the services are to be expected. Ideally, all messenger and video services operating in Germany or Europe should be included in a rating in order to achieve a high level of data protection **across the board.** It may be necessary to decide in this context whether participation in the rating procedure should be voluntary or mandatory.

---

[358] Cf. *S&P Global*, available at: https://www.spglobal.com/ratings/en/.

[359] Cf. *Moody's*, available at: https://www.moodys.com/.

[360] Cf. *Fitch Ratings*, *Inc.*, available at: https://www.fitchratings.com/.

[361] Within such a rating procedure, the data protection risk as a whole presents itself as a measurable gradual quality feature that results from the weighted evaluations of individual criteria. For some of these criteria, a gradual yardstick may also make sense, for example in the implementation of end-to-end encryption. For other criteria, such as data storage, only the option "violation" or "fulfilment of the legal requirements" seems to be appropriate.
legal requirements" is conceivable, which enters the scoring model with an appropriate evaluation.

2. Starting points for an information instrument in consumer protection

To the Bundeskartellamt's knowledge, no rating for data protection risk has yet been established in Germany or internationally.

Individual elements of a rating model are implemented for the food sector in the so-called **Nutri-Score**, which is a scoring model with a picture symbol. The label was designed by independent scientists. It is intended to help consumers to recognise at a glance, for example, which of two mueslis is the healthier choice. For this purpose, the **Nutri-Score** provides information about the nutritional value of a food on the basis of a 5-level colour scale from A to E. The energy content and the nutritional content of the food are indicated in the **Nutri-Score. The** energy content and the contents of nutritionally favourable and unfavourable nutrients are offset against each other and assigned to the scale - from A (dark green) to C (yellow) to E (red). The colours green to red help with orientation: a green A is more likely to contribute to a healthy diet than a red E.[362]

Interested food companies can use the Nutri-Score free of charge. All they have to do is register with the French brand owner, "Santé publique France", an authority in the portfolio of the French Ministry of Health, and agree to the user agreements. Companies and their brand(s) to be labelled with the Nutri-Score register on an online portal. The Nutri-Score is a voluntary statement on the front of a food product. It complements the already existing mandatory labelling elements, especially the nutrition table. The use of extended nutrition labelling models, of which the Nutri-Score is one, is regulated **uniformly throughout the EU.** Current EU law does not provide for mandatory, but only voluntary use of extended nutrition labelling at national level.

Scoring models have already been used not only in the food sector, but also for various criteria-based assessments of messenger and video services. For example, **recent publications on messenger and video services** should not be confused with a rating as described in the previous chapter. The rating system developed at the beginning of 2022 by the Foundation

[362] For example, the fibre and protein content as well as the content of vegetables, fruit, nuts, legumes and selected edible oils are classified as favourable. Energy and the content of saturated fatty acids, salt and sugar are rated as unfavourable. *Federal Ministry of Food and Agriculture*, Nutri-Score, available at: https://www.bmel.de/DE/themen/ernaehrung/lebensmittel-kennzeichnung/freiwillige-angaben-und-label/nutri-score/nutri-score_node.html.

Warentest's test procedure[363] and also the messenger investigations published by the Hong Kong Consumer Council[364] in the summer of 2021 correspond more to studies, represent a snapshot in each case and judge for the most part according to technical criteria other than those examined in this sector investigation.

Stiftung Warentest focused its investigation on functions and user-friendliness, even though individual security criteria such as encryption and essential documents such as the privacy policy were also evaluated, but with less weighting.[365] The group of participants was limited and selected by Stiftung Warentest itself. Furthermore, it is a one-off study that is not repeated on a regular or occasion-related basis. The study of the **Hong Kong Consumer Council** (consumer protection authority) was similarly oriented. According to Internet Information, the authority published a report in the summer of 2021 in which the functions and data protection of thirteen instant messaging apps were examined. Criteria included ease of use when setting up accounts, call quality, user interface, confidentiality of information and group features. The Consumer Council announced the results in its magazine "*CHOICE".* On the websites of the Consumer Council, information from the Choice journal is only available in Chinese, so a closer analysis could not be carried out. The good performance

---

[363] See *Stiftung Warentest*, Messenger apps in comparison, February 2022, available at: https://www.test.de/Messenger-Apps-im-Vergleich-4884453-0/, as of 11 May 2022. The Stiftung Warentest has tested in the areas of "functions", "set-up and use" and "privacy protection". and weighted the areas with 35%, 35% and 30%.

[364] Thirteen "instant messaging apps" were studied, including Discord, Facebook Messenger, Google Chat, Kik, LINE, Olvid, Signal, Skype, Telegram, Threema, Viber, WeChat and WhatsApp. The study said that in terms of privacy, LINE, Olvid, Threema and Signal had the highest score (5 out of 5) in the category of confidentiality when sending information. Meanwhile, WhatsApp's score was 4.5 out of 5, cf. *Consumer Council*, available at: https://www.marketing- interactive.com/consumer-council-line-and-signal-offers-highest-level-of-privacy-when-sending-data. On the websites of the Consumer Council, information from the Choice Journal is only available in Chinese, cf. *Consumer*, available at: https://www.consumer.org.hk/en/choice-magazine.

[365] All tests took place between November 2021 and January 2022. The test of functions was included in the result with 35 per cent, set-up and use also with 35 per cent and protection of privacy with 30 per cent, cf. Stiftung Warentest, Messenger - Apps im Vergleich - so haben wir getestet, available at. https://www.test.de/Messenger-Apps-im-Vergleich-4884453- 4884455/.

of leading messenger services that are particularly popular with consumers suggests that the underlying criteria did not meet what the Bundeskartellamt considers necessary.

Consumer law does not yet provide a **legal framework for** rating, or at least it has not been explicitly provided for so far. Data protection and fair trading law only oblige business transparency. The GDPR contains at least one connecting factor that can be looked at more closely. Thus, the voluntary use of data protection certificates and standardised image symbols is provided for (Art. 42, 43 GDPR) in order to prove the GDPR compliance of data processing operations. Specifically, this is evidence that the obligations to implement appropriate technical and organisational measures pursuant to Art. 24 (1), (3); Art. 25; Art. 32 (1), (3) of the GDPR as well as sufficient guarantees within the meaning of Art. 28 (1), (4) of the GDPR are fulfilled, cf. marginal no. 12.[366] In Germany, the certification bodies are now accredited by the Deutsche Akkreditierungsstelle GmbH (DAkkS) together with the independent data protection supervisory authorities pursuant to Section 39 of the Federal Data Protection Act.[367]

This procedure is unlikely to meet the requirements of a rating under Article 42 GDPR for several reasons, even if there are connecting factors. Unknown companies that are accredited as certifiers do not have the necessary **reputation to** induce messenger and video services, many of which are associated with globally leading corporations, to participate in a data protection rating. It is also questionable whether and to what extent the GDPR certification is suitable for a rating of messenger and video services because of the reference to **technical and organisational measures.** It is true that the overall context seems to capture the security criteria for messenger and video services. After all, the GDPR mentions here

"pseudonymisation", "encryption", "confidentiality, integrity, availability, resilience" of the data processing systems as well as the "recoverability of availability and access after an incident", which unfolds a certain closeness to the desired rating criteria, such as visibility of the source code, end-to-end encryption, two-factor authentication and location server. Differences, however, lie in the interpretation, as can be seen in the example of

---

[366] Furthermore, Article 63 and Article 70(1) allow supervisory authorities to submit criteria for an EU-wide certification procedure under Article 42(5) to the EDSA for approval. However, a current problem is the transfer of personal data to third countries where there is no adequacy decision.

[367] Cf. *datenschutz notizen*, available at: https://www.datenschutz-notizen.de/es-geht-voran-1-erfolge- auf-dem-langen-weg-zur-akkreditierung-nach-art-42-dsgvo-4227814/.

"encryption" becomes apparent. The GDPR addresses the risk of data misuse in the sense of data theft. Encryption is intended to make personal data inaccessible to all unauthorised persons, as is the case, for example, with hard disk and file encryption using symmetric procedures. Asymmetric encryption procedures, such as those used in end-to-end encryption, which are intended to protect bilateral data exchange, are explicitly not meant.[368]

In contrast, the **weighing factors** mentioned in the GDPR **- state of the art and implementation costs** - are also important aspects in the messenger and video services sector, which are particularly relevant when evaluating interoperability projects (cf. Chapter F.IV). In general, there is **no explicit catalogue for the technical and organisational measures according to Art. 32 GDPR, so that there** could be leeway here. Rather, the practice of IT security is familiar with various catalogues of measures, such as the BSI standards, the ISO/IEC 27001 standards or the Common Criteria, none of which have a specific focus on legal data protection requirements.[369]

Before going into concrete considerations for an assessment of the data protection risk, the advantages and disadvantages of the rating will first be briefly examined in outline from a scientific point of view in order to gain indications for a risk-minimising design.

3. Opportunities and risks from a scientific perspective

From a scientific perspective, rating agencies act as intermediaries that compile information and transform it into a rating that is made available to third parties - in this case consumers (see a)), so that they can obtain information in a more targeted manner, at lower cost and with less risk. In this way, new relationships are created between consumers, intermediaries and the services to be evaluated. In particular, these can give the intermediary and possibly the services the opportunity for opportunistic behaviour, which can, however, be prevented with the reputation mechanism (see b). The following presentation focuses on the **new information relationships and their risk-minimising handling.** For a better understanding of these, the analysis is initially carried out under the assumption of the activity of one rating authority and not several active rating authorities.

---

[368] Cf. *Simitis, Spiros, Hornung, Gerrit, Döhmann, Indra*, Kommentar zum Datenschutzrecht, Artikel 32, Rn 35, Baden Baden 2019.

[369] Cf. *Simitis, Spiros; Hornung, Gerrit; Döhmann, Indra*; Kommentar zum Datenschutzrecht, Artikel 32, Rn 78, Baden Baden 2019.

rating agencies. This also seems more obvious due to the special features of data protection risk, which is described under c).

a) Alleviate information gap

A rating could help consumers improve their level of information if services use it as a **signalling tool.** A signal is advantageous from an informational point of view if the feature of interest - in this case privacy-friendliness - is difficult to observe, while the signal - in this case the rating - is easy to observe. The latter requires, for example, that the rating is published and regularly updated.
The rating as a signal ensures a negative correlation between privacy risk and the costs of generating the rating, such as fees, information compilation and verification costs. If a service has a comparatively high privacy risk, it will receive a poor rating and face reactions from its stakeholders (complaints, churn, lower turnover, possibly higher cost of capital), especially if it is a listed company or a service affiliated with a listed group, where any news is priced in and the expectations of stock market participants play a major role. As a result, services with a high privacy risk are likely to see less incentive to conduct a rating and take the negative impact on top of the rating fees. For consumers, this means that they could infer a low data protection risk from an existing and better rating. The negative selection existing in the case of information asymmetries - as far as there is no additional information, consumers perceive all offered products as largely identical and average - can be transformed into a positive selection. For offering services, it may be worthwhile to disclose quality differences so that they are perceived. The problems of adverse selection resulting from the asymmetrical distribution of information - only average quality is perceived on the market - can consequently be mitigated by signals.[370]

[370] Cf. for the credit sector *Schaetzle* (2011), Ökonomische Funktionen von Ratingagenturen, Working Paper, Westfälische Wilhelms-Universität Münster, available at: https://www.econstor.eu/handle/10419/55765 and the literature cited there and also Cf. *Döring,* Verbraucherschutz aus Sicht der Informationsökonomik - Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, available at: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering.

Rating can also be used as part of the **screening approach**. The rating instance takes over the search and assessment of information about the messenger and video services for the consumers, which is associated with quality and cost advantages compared to many individual economic search processes. The fact that consumers use the rating as a screening indicator is tied to various prerequisites: The rating must be observable and standardised, but also differentiated enough, e.g. via categories, to be considered meaningful.[371] Above all, however, consumers must ascribe credibility and competence to the rating instance in order to
"delegate".

Rating also appears suitable for reducing risks for consumers arising from **information asymmetries after the conclusion of a contract** (so-called "hold up" and "moral hazard"). Hold up describes the "breach of promise" of a contracting party after the conclusion of a contract, because the contracting parties have concealed their aims and motives from each other before the conclusion of the contract (hidden intention, see also under G.II.2.b). Moral hazard describes the
"moral hazard", which can promote opportunistic behaviour by one of the two parties to a contract due to wrong incentives or unequal information after the contract has been concluded (cf. chapter G.II.2.b). Opportunistic behaviour can be counteracted by **incentives and corresponding measures.** From the perspective of the services, a rating should provide incentives to submit truthful information. If a company to be rated would not cooperate sufficiently, the rating authority would, for example, have the possibility to sanction this behaviour by issuing the rating opinion only on the basis of publicly available information, which would probably lead to a worse result for the company. Especially in the case of data security, many technical features are not publicly known and available. The rating authority could, for example, also withdraw a rating verdict if necessary, which could raise questions in public and have a detrimental effect on the respective service.

A rating must be adjusted immediately if new circumstances arise that could have a negative impact on the rating assessment (event-driven rating). Against this background, it could also

[371] See for the credit sector *Schaetzle* (2011), Ökonomische Funktionen von Ratingagenturen, Working Paper, Westfälische Wilhelms-Universität Münster, available at: https://www.econstor.eu/handle/10419/55765 and the literature cited there.

a so-called "watch list" is kept and published. On this list the names of
of the rating petitioners for which a change in the rating is to be expected.

b) Reputation solves "relationship problems

The rating agencies, which are active on the financial markets as information intermediaries, have already come under criticism several times in the past. During the financial market crisis in 2008, for example, they were accused of having contributed to the crisis through faulty ratings.[372] If data protection risk is to be assessed as a rating characteristic, such dramatic effects of misjudgements in ratings as in the financial markets would be unlikely. Data protection risk is not directly linked to a company's credit rating. Nor is it evident that data protection risk is a relevant factor in investment decisions. On the other hand, when it comes to assessing the default risk of a security ("creditworthiness risk") by means of a rating, this directly affects investment decisions by consumers and institutional market participants.

Nevertheless, such accusations are not surprising from a scientific point of view. When rating agencies are interposed as information intermediaries, additional **principal-agent relationships** arise as a result of unequally distributed information, **on the one hand between the rating agency and the company being rated, and on the other hand with consumers**.

Any resulting costs of monitoring and binding the agent (so-called agency costs) must be taken into account and can be controlled by designing the rating accordingly. The information between the **rating authority and consumers is** initially unequally distributed. The latter do not know the qualification and expertise of the rating instance and cannot observe its behaviour. In order to check whether a rating is factually correct, consumers would have to make time-consuming and cost-intensive efforts. This can open the door to opportunistic behaviour on the part of the rating authority. Signalling through rating then becomes

[372] Cf. *Frankfurter Allgemeine Zeitung*, Die Macht der Rating-Agenturen, 30 April 2020, available at: https://www.faz.net/aktuell/finanzen/finanzmarkt/kreditwuerdigkeit-die-macht-der-ratingagenturen-16748069.html; *ZEIT ONLINE*, Moody's fined millions for embellished ratings, 14 January 2017, available at: https://www.zeit.de/wirtschaft/2017-01/ratingagentur-moodys-millionenstrafe- finanzkrise; *Welt*, Die Rolle der Ratingagenturen in der Finanzkrise, 5 February 2009, available at: https://www.welt.de/welt_print/article3149951/Die-Rolle-der-Ratingagenturen-in-der-Finanzkrise.html, available at: https://www.welt.de/welt_print/article3149951/Die-Rolle-der-Ratingagenturen-in-der-Finanzkrise.html.

would no longer function, monitoring problems would not be solved by the involvement of the intermediary, but caused.

Information asymmetries also exist between the **rating authority and the services to be rated,** which can then also have a negative impact on consumers. Particularly when the rating agencies operate in the private sector, the question of **financing the ratings** can create dependencies. If the rating authority - in terms of financing - depends on the companies to be rated, moral hazard could arise in that

z. e.g. ratings are glossed over. Conflicts of interest are likely, especially if rating agencies also offer ancillary services (e. g . r a t i n g advisory, information events, etc.). During the global financial crisis in 2008, rating agencies are said to have become dependent on this business segment for structured financial products, which could have influenced the rating results. Private-sector rating agencies could also try to achieve higher returns not only through additional business, but also by cutting costs, by economising on the quality or timeliness of ratings and thus the necessary resources, which would ultimately harm not only consumers, but also the rated companies. After all, **confidential information is** processed in a rating process, which employees of the rating authority could use for themselves instead of letting it flow into the rating process. This

"Insider knowledge" can enable the rating authority to behave opportunistically, so that - as in the case of the aspects described above - consumers would not be better informed.[373] Corresponding **agreements on confidentiality** and **uniformity of information**

[373] Cf. on the manipulation of information also *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik - Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, available at: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering.

Specifications on the time and place of publication are thus important prerequisites for better information of the public.[374]

In order for a rating authority to achieve the goals associated with it and for information asymmetries to be reduced, the rating quality and the acceptance of the rating must be high. This is where the **reputation mechanism** can be helpful.[375] A rating authority with a reputation can thus signal to consumers that their interests are being looked after and that they can trust its judgement. It will also be inclined not to put this reputation at risk. This is especially true if it **performs** or updates **ratings on an ongoing ("multi-period") basis**, so that its future earnings depend on the quality of its judgement today.

Reputation can then lead to decreasing monitoring expenditure by consumers and services.[376]

Various measures are discussed in the literature on how reputation can be built up or enhanced. These include, for example, **concentrating on rating as the main area of business, reducing dependencies on certain companies and the exclusion of**

---

[374] On the financial markets, the legislator has established the "prohibition of insider trading" and the "ad hoc publicity" anyway, since the insider information in question - irrespective of a connection with rating - can have a direct effect on the assessment of the credit risk on the capital markets and trigger price reactions. This would not be the case with data protection information. However, the messenger and video services also include services associated with listed companies, so that it cannot be ruled out that information about possible deficits in data protection practices and the unauthorised disclosure of this information could have an impact on the refinancing possibilities of these services.

[375] Other possibilities, but less significant in this context, are the establishment of a brand name, the granting of guarantees or advertising, cf. *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik - Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, available at: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering.

[376] Cf. *Schaetzle* (2011), Ökonomische Funktionen von Ratingagenturen, Working Paper No. 113, Westfälische Wilhelms-Universität Münster, available at: https://www.econstor.eu/handle/10419/55765; *Heinke* (1998), Bonitätsrisiko und Credit Rating festverzinslicher Wertpapiere, Bad Soden, Ts./ Uhlenbruch.

Interdependencies with companies to be rated.[377] From the sovereign side, the risk that rating results are linked to regulatory obligations must be countered.
- as is the case, for example, with capital market regulation - so that ratings could turn into "**regulatory licences**" that virtually take the place of regulatory orders and their implementation. Loss of information and information control in accordance with the requirements of the regulatory authorities could be the undesirable consequences.[378] The independence of the rating judgement would be called into question. Transferred to the area of data protection, it would have to be ensured that the rating criteria are distinguished from other supervisory examination procedures and that there is no mixing. It should be noted that the involvement of a rating authority as an intermediary establishes new relationships with information imbalances, namely with the services to be rated on the one hand and with consumers on the other. Risks from opportunistic behaviour of the rating authority can be mitigated if **dependencies** are **reduced.** This concerns the way in which funding is arranged - who pays, concentration on rating as the only business area, avoiding intertwining and mixing with other tasks, viable agreements on confidentiality and on the place and time of publication of the rating, and no linkage with regulatory measures. Reputation of the rating authority can then mitigate the dangers of unevenly distributed information, especially if ratings are carried out on an ongoing basis.

c) Trust through independence

In the previous section it became clear that many **difficulties** can arise **from dependencies** on rating agencies. These come to bear especially when rating is organised in the private sector. The fact that the rating of credit risk on the financial markets is carried out by three private rating companies is due to historical development. It

---

[377] Cf. e.g. E.g. *Heinke* (1998), Bonitätsrisiko und Credit Rating festverzinslicher Wertpapiere, Bad Soden, Ts./ Uhlenbruch; Wappenschmidt (2009), Ratinganalyse durch internationale Ratingagenturen, Frankfurt am Main.

[378] Cf. *Partnoy*, The Siskel and Ebert of Financial Markets?: Two thumbs down for the credit rating agencies, in: Washington University Law Quarterly, vol. 77, issue 3, available at: https://journals.library.wustl.edu/lawreview/article/id/5968/ and also Cf. *Frankfurter Allgemeine Zeitung*, Die Macht der Rating-Agenturen, 30 April 2020, available at: https://www.faz.net/aktuell/ finanzen/finanzmarkt/kreditwuerdigkeit-die-macht-der-ratingagenturen-16748069.html.

The capital market began in the 19th century in the USA, where the nationwide spread of the railways triggered a high demand for financing. The capital market that was established for this purpose was largely anonymous and intransparent, so that lenders were exposed to a high credit risk.[379] After two entrepreneurs initially collected and published relevant information, they founded the well-known rating agencies at the beginning of the 20th century, which are still active today. Institutional investors have a high interest in not investing in securities with a low credit rating and use ratings to reduce their risks, which they could not do themselves in such a way.

For the data protection risk, it seems less sensible to commission profit-oriented companies. It is not to be expected that the services are willing to finance such a rating. Their data protection activities have so far apparently been less relevant to success than other competences.

Therefore, opportunities for private rating providers to earn money do not seem to open up for the time being. Private providers would also need to have not only the relevant competencies but also the necessary reputation to mitigate the information problems described above (see G.III.3.b).

A governmental body or one that is otherwise independent of profit interests would have to have the necessary reputation, in addition to the corresponding professional aptitude, in order to gain the trust of services and consumers in the quality of the rating.

Essential criteria here are independence in decision-making and no mixing with other, e.g. regulatory tasks, as outlined in the previous section c).

4. Special suitability for data protection practice

Unlike many other information-related measures, the rating is not only aimed at one side of the market, i.e. either the messenger and video services as providers on the one side or the consumers on the other. Rather, it is likely to affect both sides

- both the services and their users - to be more proactive. Furthermore, a comparison of the efforts of implementation with the long-term positive effects suggests that the benefits will clearly outweigh the costs. Finally, as far as the scope of a rating is concerned, different design options are conceivable

A rating can be a **motivation for both sides of the market**. However, based on the findings so far in this sector enquiry, the use of a **rating as a signal** of data protection risk may be more promising in practice than relying on its effect as a screening indicator for the

[379] See *Wikipedia*, available at: https://de.wikipedia.org/wiki/Rating.

privacy features of a messenger and video service. While in screening the uninformed side of the market - the consumers - tries to eliminate the information gap, in signalling the better informed side provides information on its own initiative. More than the consumers, the messenger and video services could be sensitive to published data protection risk information, especially if vague assumptions and criticisms of their data protection practice are replaced by a publicly examined judgement.

become. Data protection is not only "law" - in Germany and Europe in the form of the GDPR - but has also become a sensitive topic that is closely followed by the (professional) public and also attracts attention in the political environment. The constant confrontation with the practices of some leading industry representatives and public reflection on government initiative due to undesirable practices and developments have also contributed to this. It is therefore reasonable to assume that many messenger and video services would like to avoid a **publicly negative report card or a worse ranking than their main competitor.** Finally, in the case of listed companies, effects on financing costs cannot be ruled out. However, it is also conceivable that consumers do not want to be registered with a messenger and video service that comes **last** in **the ranking.** Perhaps one of their contacts would also prefer to use a messenger and video service that has a lower data protection risk than the service they have chosen so far. A published rating from a trustworthy authority could be the **credible information that professional users need.**

"Decision-makers" or contact persons for the public at authorities and companies need to decide on the GDPR compliance of a messenger and video service and thus its possible use in their own institution.

All in all, resources must be spent on promoting data protection as a competitive parameter on the state side.

Conversely - in the current situation without a rating - the **deficits in the market mechanism that** exist and persist due to the current information asymmetries are also not without monetary consequences. The overall **welfare losses to date,** or even just the costs of public sector proceedings based on competition, data protection and regulatory law against leading industry participants, are likely to be substantial. If messenger and video services, on the one hand, and consumers, on the other, included data protection as an important criterion in their decisions, undesirable developments in the data protection practices of individual industry representatives - as discussed in public - could also be turned in the right direction in the future.

In addition to the question of overall economic costs, for a practical implementation it must be considered on which **political-administrative level** - worldwide, EU-wide or national - the rating should be implemented. As has been described several times in this report, the industry of messenger and video services is very diversely positioned and includes a wide range of companies and free applications with **different regional focuses and ranges**. Some large services are used by consumers worldwide and many other services are also active in several world regions. Therefore, a globally uniform rating procedure for data protection risk would ideally be advisable. Quite apart from problems of international coordination and harmonisation, however, the different data protection legal frameworks between the various jurisdictions are likely to stand in the way of such a globally uniform rating system. Therefore, an implementation at the European level within the **scope of the GDPR** might be closer**.**

H. Recommendations

In addition to the results of its investigations and their legal classification, the sector enquiry into messenger and video services provides important information on how to deal in future with the situation in messenger and video services, which in some cases is unsatisfactory under consumer law. Due to the diversity of the sector and the many business models and free applications in addition to the well-known market leaders, the Bundeskartellamt would like to use this report to contribute to more transparency and thus provide concrete indications for improvements in consumer protection that are beneficial to the economy as a whole.

In order to make data protection in messaging and video conferencing more widespread, the consumer-friendly handling of user data should be promoted as a competitive parameter in messenger and video services. Various measures could be taken to achieve this (see Figure 18).

First of all, consumer law enforcement should be strengthened and aligned with the requirements of the digital economy (see I.). In addition, consumer education should not only be intensified, but also condensed and better adapted to their needs (see II.). In addition to caring for consumers, it should not be neglected to create better competitive conditions for data protection-friendly services, which can be achieved by relatively simple means (see III.). Up to now, consumers have not been able to access compressed information on the data protection quality of their services, such as could be produced by a rating procedure. Therefore, when designing interoperability projects, care must be taken that they are not only introduced in an innovation-friendly way, but also in a consumer-oriented way (on basic conditions under IV.).

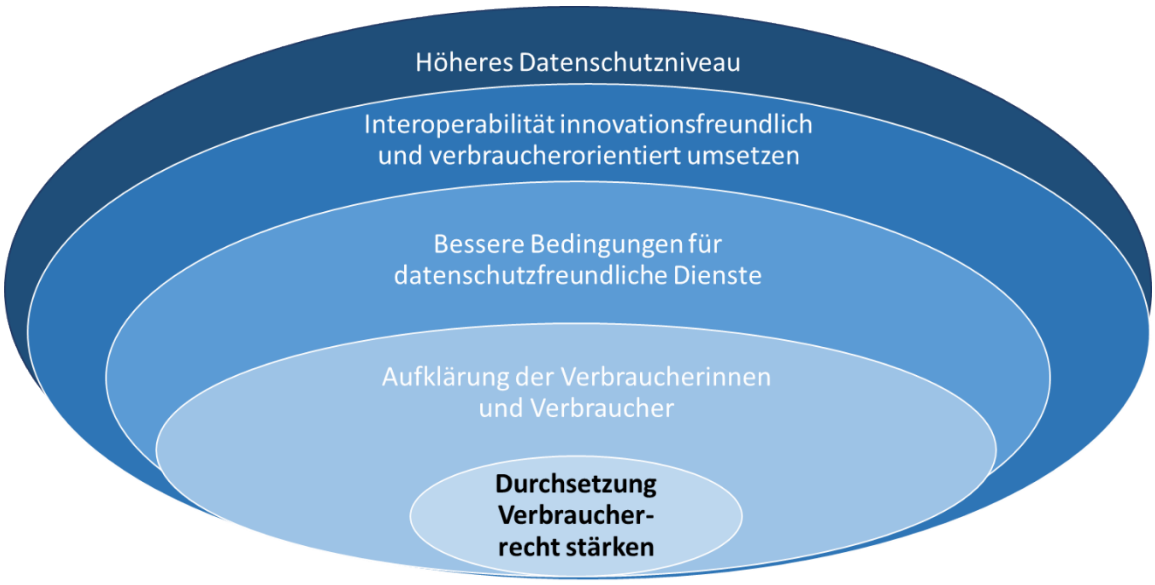


Figure 18: Recommendations for action for a higher level of data protection

I. Strengthen enforcement of consumer law

The Bundeskartellamt investigated three legal issues that are particularly important for consumers in messaging and video conferencing. The practices investigated were suspected not only of endangering data security but also of resulting in consumer rights violations.

This suspicion could not be dispelled in two of the three fields of investigation within the framework of this sector enquiry; in the third field of investigation, at least the impression remained that improvements in the provision of information are necessary for the benefit of consumers (see under 1.).

The same applies to the enforcement of consumer law. The digital economy poses ever new challenges, especially due to its technical basis. Regulatory enforcement can make a meaningful contribution to managing and shaping these challenges (see 2.).

1. Consumer law infringements and legal risks

Synchronisation of the contact directory

The common practice of many well-known messenger and video services to upload and synchronise the contact directory of users also leads to the contact data of non-users being collected. They cannot consent to the synchronisation pursuant to Art. 6 (1) subpara. 1 a) DSGVO. The synchronising service is not known to them. The responsibility under data protection law cannot be shifted to the user, but lies with the respective service itself. The telephone number of the non

The personal data of the user or non-user is personal data within the meaning of Art. 4 No. DSGVO, even if no other data is collected apart from the telephone number. The personal reference also continues to exist if the telephone number is replaced by a cryptographic hash value linked to the user from whose contact directory the telephone number originates. The service would thus need a different legitimisation for data processing - i.e. long-term telephone number storage of non-users. It cannot be expected that this would arise from the protection of legitimate interests (Art. 6(1), subpara. 1, letter f DSGVO) of the data controller, which must be weighed against the liberties of the data holder concerned. The networking advantage appears to be too small, especially in terms of time, assuming daily synchronisation. Only the short-term uploading of telephone numbers and the subsequent deletion of those numbers of non-users may constitute a legitimate interest.

International data transfer / data storage

The results of the investigation into the data processing process suggested that some messenger and video services were not behaving in a legally compliant manner when transferring data to third countries and storing it on servers in third countries (Art. 45 GDPR). This primarily concerned those services that store data of German users in the USA. In addition, other services maintain server infrastructures in the EU and third countries, especially the USA. It remained unclear where data of EU citizens was transferred to. This was partly dependent on various constellations. In the case of free messenger clients, the location of data storage depends on the user's choice of server.
Data may only be transferred to countries outside the EU and the European Economic Area if an adequate level of data protection is ensured in the respective third country (Art. 45 GDPR). However, the former data protection shield (EU-US Privacy Shield), which the EU had negotiated with the USA, is invalid after the "*Schrems II*" ruling of the ECJ from summer 2020. Unless the controllers within the services have meanwhile based their data transfers to countries outside the European Union on a new basis, such as appropriate safeguards including additional measures, if necessary, the data transfer would be unlawful. This suspicion could not be dispelled for the majority of services, as there is no information on concrete safeguards.

Information deficiencies in connection with end-to-end encryption

The Bundeskartellamt had chosen end-to-end encryption for a legal analysis for several reasons.
For example, encryption, as a complex technical topic for the layman, is an example of the far-reaching informational disadvantages of consumers

consumers. The notion of end-to-end encryption had also been publicly associated with security shortcomings, not only on the merits, but also as an example of the particular challenges that can come with interoperability.

For a violation of the duty of transparency under unfair competition law, it would have to be proven whether information on the security of the communication, such as the use of a special encryption method, is to be assessed as material within the meaning of Section 5a (1) UWG, whether the withheld information is necessary for making an informed business decision and whether it can be suitable to influence the decision of the users of a messenger and video service in such a way that they might have decided differently if the relevant facts had been disclosed.

In the Bundeskartellamt's view, a **transparency violation** will not be easily justified **by information deficiencies regarding the** type of encryption, even if certain **legal risks** exist. It is true that not only security features corresponding to the extensive provision of information by the services can be counted as "essential information". The unclear, incomprehensible or ambiguous provision of information by many messenger and video services could also be declared as "withholding". In contrast, however, the

"**business relevance**" of the security features will be difficult to justify. Market development has progressed. End-to-end encryption has established itself as an industry standard, so it probably makes no difference where users register in terms of this security feature. (Even though against this background it was surprising that a few well-known services do not implement end-to-end encryption or only to a limited extent). A better assessment of the consumer perspective would have required further investigative effort such as a consumer survey, with which, however, only uncertain chances of clarification were associated due to the complexity of the terminology. The classification of consumer behaviour from the company's point of view also remained ambiguous, as there are many free offers of messenger and video services. In the end, a conclusive assessment had to be left to **clarification in** each **individual case.**

2. Law enforcement - stocktaking and perspectives

In any case, the initial situation of **consumers** in enforcing their rights is not easy, since it is generally not worthwhile for them to sue in the case of data protection problems. Furthermore, it can be observed that individual judgements are only transferred with difficulty to the entirety of consumers. The fact that this results in a so-called

"rational apathy" develops, i.e. the decision not to invest due to too much effort compared to the Not taking action is not surprising given the likelihood of success.

In addition, the actors of proven private law enforcement are faced with **new requirements in** matters from the **digital economy.** Due to the great influence of technical circumstances on the data protection quality of messenger and video services, the proof of legal violations can generally be challenging for **associations in** complex cases from the digital economy. This is especially true when there is no access to technical information because it is held by the companies. In contrast to less technically based questions, no reliable conclusions can be drawn about legal violations. **Official procedures** would then be the means of choice to collect the information directly from the companies, as the Bundeskartellamt did in the context of this sector enquiry.

As far as violations of **fair trading law** and civil law are concerned, there has been no enforcement by public authorities so far anyway. Consumer protection regulations in these areas of law are traditionally enforced by private plaintiffs in Germany. However, even in the **enforcement of data protection law,** surveyed messenger and video services see a need for an expansion of official enforcement. While the GDPR was well received as a set of rules, the organisation at European level and the rules on jurisdiction were viewed critically. This is because in the case of cross-border data processing, the data protection authority at the headquarters of the controller is the lead authority. If procedures accumulate at individual data protection authorities, the large **mass of GDPR violations** could become an obstacle to enforcement.

Messenger and video services are not only active in Germany and Europe, but are often globally networked. Accordingly, German law enforcement actors have to deal with the **internationality of the industry,** as the comments on international data transfer demonstrate.

II. Continuous education of consumers

As the investigation results in the previous chapter have shown, there is a consensus among the services that consumers need to be further educated and informed. There must be clearer, more practical and continuous information about the protective handling of personal data. This includes, for example, knowledge about how to check the trustworthiness of IT systems. The **development of media literacy** is a long-term endeavour that should begin in primary school and continue until students enter training and higher education. All population groups should be integrated into a **communication strategy for data protection.** Here, the information channels that consumers prefer to use, namely internet-based digital media, could be used. The less internet-savvy population groups could additionally be reached via conventional media, such as television. Nationwide continuous campaigns are largely lacking so far.

The behaviour of **public decision-makers** also has an influence. This concerns in particular those institutions that have a high degree of penetration and enter into direct digital contact with consumers, such as public television and radio, but also individual authorities, cities and municipalities. It should be examined whether privacy-friendly messenger and video services can be increasingly used for contact. The way messenger and video services themselves **inform** their users about **data security and data protection** should also be improved in terms of content, presentation and communication in order to reduce search costs for consumers.

III. Better conditions for privacy-friendly services

The situation of privacy-friendly messenger and video services could already be improved with comparatively little effort. This concerns both investments in data protection-friendly services - i.e. their selection and paid use in the public sector - and a review of the promotion of open source developments. Here, too, the need for better **targeted information provision is at the** forefront of all aspects.

Reliable **information on the GDPR compliance of messenger and video services** - especially those services that are not in the focus of public interest - is hardly available publicly. It is possible that targeted information - as would be generated by a rating of the data protection risk - about the members of the industry and their data protection competences could also lead to improvements in the **design of tenders.**

As far as the **promotion of open source is concerned**, there is apparently also a lack of reliable and easy-to-find information, here for the interested services. According to industry representatives, it would be helpful to have an **overview in the form of a European or German website** where all funding opportunities and the respective funding criteria can be presented and viewed. The general public would benefit from open source developments without persistent bugs that affect data security and data protection, as the developments are open to all interested parties. Therefore, it could be beneficial for data protection if the current funding spectrum, which is geared towards new developments, were to be expanded. It could have a positive effect on data security if **maintenance and care of** the open source software, including troubleshooting and bug fixes, as well as the operation of the necessary hardware and its maintenance, were also included in funding programmes.

IV. Implementing interoperability in an innovation-friendly and consumer-oriented way

As the Bundeskartellamt discussed in the interim and final report, any project to implement and design interoperability must take into account **effects on innovation and competition, for** example when the necessary standardisations meet different technical designs of the services. It is true that the DMA interoperability regime is limited to basic functions and is asymmetrically designed. However, the architecture of the services and the technical location of the individual functions on it are very individual, so that interoperability here would require standardisations and adaptations to varying degrees. This could also affect the innovative forces of the services differently.[380]

However, the **perspective of consumers who** use messenger and video services must also be taken into account. Up to now, consumers have not been able to fall back on the results of rating procedures or similar methods when they are looking for concise and comparative information about the data protection quality of messenger and video services (see again under G.III.) If interoperability were to be practised between individual services or in larger groups in the future, the information situation could become even more opaque for users. The desire associated with interoperability to weaken network effects and to give data protection-friendly services better chances in competition by consumers switching could thus be thwarted.

Consumers must therefore not be left to their own devices. Data protection and data security must be taken care of. Any **plans to implement and design interoperability** and to **overcome the technical challenges** must keep the security and protection of the data of all consumers in mind and include all the services they use. Due to the interdisciplinary challenges in the area of messenger and video services - information technology, consumer and data protection law as well as economic - a **cooperation of different knowledge carriers in** such interoperability projects seems to make sense. In view of the dynamism of the sector and the innovation potential of the technology, it appears to be

---

380 An in-depth technical presentation of the possibilities of end-to-end encryption under interoperability is provided by the BNetzA study "Interoperability between Messaging Services - Secure Implementation of of Encryption", April 2023, available at: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteropEncryption.pdf?_blob=publicationFile&v=1. The study involves seven messenger and video services and is based on an examination of publicly available technical documentation and scientific publications.

As already mentioned in the interim report, it would be advisable to involve the industry, as has already been done in principle by the European Commission at a workshop on interoperability in February 2023.

Since the industry - as emphasised at various points in this final report - is diverse in technical and commercial terms, any rules on technical implementation should be **non-discriminatory as long as the state of the art is guaranteed.**

As this research has shown, consumers have **choices in** many messenger and video services as to whether or not to set certain features. For example, consumers can decide whether or not to enable end-to-end encryption. Many services also offer different versions of their app, where different functions can be used depending on the fee. The extent to which this also entails different levels of security criteria, for example transport encryption or end-to-end encryption, is often not clearly recognisable. For a secure **consumer product under interoperability,** it would be important that a corresponding regime provides for already activated security criteria to be preserved in cross-messenger exchange.

Furthermore, **data** should also be **processed sparingly** under interoperability. In this investigation, the Bundeskartellamt particularly emphasised the question of server location, the type of business model and the handling of contacts. Messenger and video services must store data of European users in the European Union in order to comply with the European GDPR. The data of users is considered better protected in this legal framework than, for example, in the USA. The **business model** as a first indication of the intensity of data transfer can perhaps still be used by users for the service they use directly. Under interoperability, with the involvement of other services, **data sharing and utilisation** may no longer be easy to oversee. Some messenger and video services are linked to large corporations that rely on neighbouring services.

business fields hold strong positions and maintain a "digital **ecosystem**". Internal sharing of user data could already be widespread here without cross-messenger exchange. Many of these services can only be used if users create accounts that are used for different functions. In some cases, consent to the processing of data from other services has also been assumed up to now.

Finally, how the services handle the users' **contacts is** just as essential for the quality of data protection, since the users not only take responsibility for their own data, but also for the data of third parties. It should be possible to maintain a clearly protective approach even under interoperability.

Appendix: Included services and glossary

Included services

Adobe Connect / connect@reflact	All-in-one	BigBlueButton
Blabber.im	Conferencing & Collaboration	Conversations
Delta Chat	Dino	Discord
Element	Facebook Messenger	Fastviewer
Franz	Gajim	Ginlo
Google Meet	GoToMeeting	GoToWebinar
iMessage/FaceTime	Jabber	Line
Loopup	Meet.jit.si	Monal
Nextcloud Talk	Profanity	Quicksy
Rocket.Chat	Skype	Slack
Snapchat	Swyx	(Microsoft) Teams
TeamViewer Meeting	Threema	Tixeo
Trillian	Univado	Viber
Webex	WeChat	WhatsApp
Yaxim	Zoom	

Glossary

Term	Definition
ACCC (Australian Competition and Consumer Commission)	Australian Competition and Consumer Commission.
AES (Advanced Encryption Standard)	Symmetric encryption method that was standardised by the National Institute of Standards and Technology (NIST) in 2000 and is one of the most widely used symmetric methods today.
API (Application Programming Interface)	Programming interface; programme part that is made available by a software system to other programmes for connection to the system.
App (from English application):	Application software (i.e. an executable programme) that fulfils a useful function but is usually not relevant to the functioning of a system as such.
Asymmetric procedure (public key procedure)	Cryptographic procedure in which each participant generates a key pair consisting of a private key, which is used to decrypt or sign data, and a public key, which can be used to encrypt or verify signatures. The private key must be kept secret and it must be practically impossible to calculate it from the public key.
Augmented reality (augmented reality, AR)	Interaction of digital and analogue life via the camera of the smartphone or via glasses, whereby these do not completely seal off the user from his normal environment like VR glasses. Instead, additional information about their surroundings is superimposed on the glasses.
Authenticity	One of the four security goals of cryptography, which states that the originator of data or the sender of a message should be clearly identifiable and its authorship verifiable.
Backward Secrecy, Future Secrecy (Post-Compromise Security, "self-healing")	Property of a cryptographic protocol that guarantees that encrypted messages remain secret even after a key has been compromised in the past.
BEREC (Body of European Regulators for Electronic Communications)	BEREC is intended to bring about greater coordination of the respective national regulatory practices by applying the European regulatory framework for electronic communications networks and services as uniformly as possible in order to promote the further development of the internal market for this sector.
BfDI (Federal Commissioner for Data Protection and Freedom of information)	Independent, independent supreme federal authority for data protection and freedom of information.
BNetzA (Federal Network Agency)	Higher German federal authority and regulatory authority with the central task of promoting competition in the energy, telecommunications, postal and railway markets and ensuring the performance of the infrastructures in these areas.
BSI (Federal Office for Information Security)	Federal cyber security authority and, as a German higher federal authority in the portfolio of the Federal Ministry of the Interior, for Construction and Home Affairs, responsible for information security for the state, the economy and society.
Client	Programme or application which is installed on the terminal of a network. is executed and communicates with a server (central computer).
CMA (Competition and Markets Authority)	UK Competition and Markets Authority.

Term	Definition
Common Criteria (CC)	International standard for testing and evaluating the security properties of IT products
Data portability	The portability of personal data.
Data processing	A variety of different processes carried out with or without the help of automated procedures in connection with personal data (according to Art. 4 (2) GDPR). Used here as a generic term for data collection, data use, data disclosure, data storage and data deletion.
Deniable encryption	Encryption technique in which the existence of an encrypted file or message can be denied in the sense that a counterpart cannot prove that the plaintext exists.
(Plausible) **Deniability** (plausible deniability)	Property of a cryptographic protocol which enables the The fact that the message has been sent can be credibly denied afterwards.
DMA (Digital Markets Act, Ordinance on Digital Markets)	The Digital Markets Act (Regulation (EU) 2022/1925) aims to ensure contestability and fairness of markets where large online platforms operate, which are operated by "gatekeepers" are provided. Together with the Digital Services Act, it is one of the core elements of the EU Digital Strategy.
Double Ratchet Protocol	Cryptographic protocol for asynchronous (i.e. the communication partners do not have to be online at the same time) end-to-end encrypted message exchange.
DSA (Digital Services Act, Ordinance on Digital Services)	The Digital Services Act (Regulation (EU) 2022/2065) aims at a safe, predictable and trustworthy online environment in which innovation and in particular the principle of consumer protection are promoted. Together with the Digital Markets Act, it is one of the core elements of the EU Digital Strategy.
GDPR (General Data Protection Regulation)	EU regulation that governs the processing of personal data of natural persons by natural persons, companies or organisations in the EU.
DTLS (Datagram Transport Layer Security)	Security protocol based on the functionality of TLS (Transport Layer Security). In contrast to TLS, DTLS does not use the secured, connection-oriented transport protocol TCP, but the unsecured UDP (User Datagram Protocol) for the encrypted and protected transmission of data.
EKEK (European Electronic Communications Code)	EU Directive regulating electronic communications networks and services.
Encryption at Rest	Storage encryption; encryption of data (so-called data at rest, as opposed to data in transit and data in use) that is stored in some form in the memory of a computer/terminal device.
End-to-end encryption (End-to-End Encryption)	The encryption of transmitted data across all transmission stations. Only the communication partners as end points of the communication can decrypt the data.
(Perfect**) Forward Secrecy** (inconsequentiality)	Property of a cryptographic protocol that makes it impossible to reconstruct a session key by knowing a secret master or long-term key. A recorded encrypted communication can thus not be decrypted retrospectively even if the long-term key is known.
BEREC (Body of European Regulators):	See BEREK.

Term	Definition
GSM (Global System for Mobile Communications)	Mobile radio standard for fully digital mobile radio networks, which is mainly used for telephony, but also for circuit-switched and packet-switched data transmission as well as short messages. First standard of the so-called second generation ("2G") as successor of the analogue systems of the first generation (in Germany: A-network, B-network and C-network).
ARC (Act against Restraints of Competition)	Basic law of the market economy and the central legal basis for the work of the Bundeskartellamt. The object of protection of the ARC is competition in the Federal Republic of Germany, which is to be protected against any restriction, irrespective of whether it was caused domestically or abroad.
Identifier (Client) ID	Describes the characteristic of a messenger service user, which is their allows unambiguous identification.
IEEE (Institute of Electrical and Electronic Engineers)	Worldwide professional association of engineers mainly from the fields of electrical engineering and information technology, which, among other things, forms committees for the standardisation of techniques, hardware and software.
IETF (Internet Engineering Task Force)	Open, international voluntary association of network engineers, manufacturers, network operators, researchers and users concerned with the technical development of the Internet - in particular standardisation of the communication protocols used on the Internet - in order to improve its functioning.
IMAP (Internet Message Access Protocol)	Network protocol that provides a network file system for e-mails. With IMAP, e-mails remain stored on the server and can thus be retrieved from several devices.
Contents	Texts, speech, video, photos, saved or sent files.
Interoperability	Refers to the capability of independent, heterogeneous messaging systems or Messenger clients to be able to collaborate to varying degrees.
ISO (International Organization for Standardization)	The International Organisation for Standardisation is the international association of standards organisations. It develops international standards in all areas except electrics, electronics and telecommunications. It is part of the WSC (World Standards Cooperation).
Key Pinning	Mechanism to secure the HTTPS protocol against man-in-the-middle attacks with forged certificates signed by a recognised certificate authority.
Messenger service	Collective term for open and closed messaging systems, messenger clients and multi-messengers that offer messaging functions and/or video telephony (individually and/or in groups, such as in video conferences, online meetings, webinars, etc.).
Messaging Layer Security (MLS)	Messaging protocol based on the Double Ratchet protocol and standardised within the framework of an IETF working group. The standard aims to improve group management and the interoperability of different messengers.
Messaging system	Collective term for the entire system required for messaging, consisting of communication protocol, user software (app, client), server software and hardware.
MIMI (More Instant Messaging Interoperability) Working Group	IETF working group working on solutions for interoperable messaging, which met for the first time in spring 2023.
Multiprotocol Clients / Multi (Protocol) Messenger	Software that masters a wide range of communication protocols and The use of different communication services via one interface.
User	Collective term for organisers and participants who use a Messenger or Use video service.

Term	Definition
OpenPGP	Standardised data format for encrypted and digitally signed data. Also defines the format of certificates, commonly referred to as "keys".
Open Source	Software, the source code of which is publicly and by third parties viewed, changed and can be used.
Organiser (Ersteller, Erstellering, Administrator, Administratorin, Host)	Collective term for a person or institution that can actively start an exchange via text messages, telephony or video telephony and invite other participants to it, as well as possibly have further authorisations (e.g. muting participants, deleting groups, removing participants, etc.).
OTR protocol (Off-the-Record Protocol)	Protocol for message encryption in instant messaging (i.e. the communication partners must be online at the same time), which is considered the predecessor of the Double Ratchet Protocol.
OTT (Over the Top)	Content that is offered via an internet connection without the internet providers themselves having influence or control over the content, so that OTT services are decoupled from the infrastructure providers.
Peer-to-peer	Communication among equals (related to a computer network). Is used here used for direct communication between two users.
Personal data	According to Art. 4 No. 1 of the GDPR, this is all information that relates to an identified person. or identifiable natural person.
POP (Post Office Protocol)	Transmission protocol via which a client can fetch e-mails from an e-mail server. With POP3, the e-mails are fetched from the server and are then only stored locally in the user's e-mail programme. POP3 can therefore be used with only one device.
Proprietary	Software and hardware that is based on manufacturer-specific standards, is distinct from free (open source) software and hardware and also does not allow external, public intervention.
(Communication) **protocol**	Rule set according to which the data transmission between two or more end points.
RFC (Request for Comments)	Collection of numbered documents published by the IETF. RFCs deal with protocols, methods, programmes and concepts that are indispensable for the cooperation of different systems on the Internet.
RTSP (Real-Time Streaming Protocol)	Network protocol for controlling the continuous transmission of audiovisual data (streams) or software over IP-based networks.
RSA (Rivest-Shamir-Adleman)	Asymmetric cryptographic procedure that can be used for both encryption and digital signing.
SEP (Standard essential patents)	Patents for inventions that are an essential part of a standard.
SIP (Session Initiation Protocol)	Network protocol for establishing, controlling and terminating a communication session between two or more participants.
S/Mime (Secure/Multipurpose Internet Mail Extensions)	Standard for the encryption and signing of MIME objects using a hybrid cryptosystem. S/MIME is used in many protocols to secure the application layer, typically for e-mail.
SMS (Short Message Service)	Telecommunication service for the transmission of text messages, usually called short messages or also SMS.
SMTP (Simple Mail Transfer Protocol)	Protocol of the Internet protocol family used for the exchange of e-mails in computer networks. It is primarily used for sending and forwarding e-mails.
SRTP (Secure Real-Time Transport Protocol)	Encrypted variant of the Real-Time Transport Protocol (RTP).

Term	Definition
SSO (Single Sign-on)	After a one-time authentication at a workstation, users can access all computers and services for which they are locally authorised from the same workstation without having to log in to the individual services each time.
SSL (Secure Sockets Layer)	Predecessor of Transport Layer Security (TLS); encryption protocol for secure data transmission on the Internet.
Symmetric method (cryptography)	Cryptographic procedure in which the key for encryption and decryption is identical and must be exchanged beforehand between the communication partners.
Participant, Participant	Collective term for a person or institution that can only participate in an exchange via text messaging, telephony or video telephony (individually or in groups) at the "invitation" of an organiser.
TLS (Transport Layer Security)	Encryption protocol for secure data transmission on the Internet, further development of Secure Sockets Layer (SSL).
Transport encryption (point-to-point encryption)	Term for sending unencrypted data via an encrypted channel. Outside the transmission path and at the end points, the data is unencrypted.
Video service	Collective term for systems and applications of video telephony (individual and/or groups, such as in videoconferences, online meetings, webinars etc.) and, if applicable, messaging functions (individually and/or in groups).
Virtual Reality (virtual reality, VR)	Digital image of reality created on the computer.
WebRTC (Web Real-Time Communication)	Open standard that defines a collection of communication protocols and application programming interfaces (API) that enable real-time communication over computer-to-computer connections.
W3C (World Wide Web Consortium)	Body (member organisation) for the standardisation of techniques on the World Wide Web.
XMPP (Extensible Messaging and Presence Protocol)	Open standard of a communication **protocol** published by the Internet Engineering Task Force (IETF) as RFC 6120, 6121 and 6122.
XSF (XMPP Standards Foundation)	Non-profit foundation that specifies and further develops the XMPP protocol.
Two-factor authentication	Proof of identity of a user by means of the combination of two different and in particular independent components (factors), such as password and fingerprint.