Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

SHORT NOTE

on the proposed new UK data protection regime & on the continuing UK surveillance regime

Attachment 2: Background and selected detailed analyses

Introduction

This attachment to the Short Note on the proposed new UK data protection regime & on the continuing UK surveillance regime provides more detailed legal background to the Data Protection and Digital Information Bill discussed in that note, and examples of more detailed analyses of two important matters covered by the Bill: the definition of "personal data" and the issue of "lawfulness and purpose-limitation". The aim is simply to show the complexity of the law and of the issues addressed in the Bill: there was no time to write up my analyses of all the issues covered in my Short Note.

1. The UK data protection regime

The development of the UK data regime – or rather, regimes – over time is well summed up in the UK government's Explanatory Notes to the Data Protection and Digital Information Bill:[1]

> The UK is a party to the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", which became open for signature in 1981. Parliament passed the Data Protection Act 1984 to ensure compliance with the standards set out in the Convention and ratified the Convention in 1985.
>
> The Data Protection Act 1984 was repealed and replaced by the Data Protection Act 1998, which implemented the EU Data Protection Directive (95/46/EC) ("the 1995 Directive").
>
> The 1995 Directive was replaced by the EU General Data Protection Regulation (2016/679) (the "EU GDPR"), which applied directly in the UK from 25 May 2018. This was supplemented in the UK by the Data Protection Act 2018 ("DPA 2018") (in particular in Part 2 of the Act), which repealed the Data Protection Act 1998 and exercised derogations provided by the EU GDPR.
>
> The EU GDPR does not apply to processing by competent authorities for law enforcement purposes. Such processing is subject to EU Directive 2016/680, which was transposed into UK law in DPA 2018 (in particular in Part 3 of the Act).
>
> The DPA 2018 provides for a further processing regime for processing by the Intelligence Services (in Part 4 of the Act).
>
> The EU GDPR was incorporated into UK law at the end of the EU Transition Period under section 3 of the European Union (Withdrawal) Act 2018 (EUWA 2018) and modified by the Data Protection, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019 under the power in section 8 EUWA 2018 to create the UK GDPR.
>
> The UK's data protection framework therefore comprises three regulatory regimes:
>
> - general processing of personal data - governed by the UK GDPR as supplemented by Part 2 of the Data Protection Act 2018;
> - processing by "competent authorities" (as defined in section 30 & schedule 7 DPA 2018) for law enforcement purposes - governed by Part 3 DPA 2018, which implemented EU Directive 2016/680 (the EU Law Enforcement Directive) into UK law;

- processing by the UK intelligence services - governed by Part 4 DPA 2018.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 transposed Directive 2022/58/EC. These contain some special rules for certain types of processing, such as personal data collected through cookies and direct marketing, which overlay the general rules for processing in the UK GDPR.

The Data Protection and Digital Information Bill makes various amendments to these existing sources of data protection law.

In other words, if the Bill is adopted, the UK data protection regime will continue to be formed by the DPA 2018 and the UK GDPR, but both will then apply as amended by the DPDI Bill.

2. The DPDI Bill

The UK Government published the Data Protection and Digital Information Bill on 18 July 2022.[2] As the government itself put it:[3]

> **This primary legislation will harness our post-Brexit freedoms to create an independent data protection framework.**

These "post-Brexit freedoms" are to be used with clear aims:[4]

> This government's ambition on data is clear: **we will establish the UK as the most attractive global data marketplace**. …
>
> The reforms we are taking forward will help the UK **realise the benefits of greater personal data use**. We are **reducing the burdens on businesses that impede the responsible use of personal data**. … We will also **make it easier for businesses to use automated decision making tools responsibly** …
>
> **The reforms proposed in the consultation provide an opportunity for the UK to reshape its approach to regulation outside of the EU, and seize opportunities with its new regulatory freedoms. This includes the use of repatriated 'adequacy' powers from the EU to remove inappropriate barriers to the flow of UK personal data overseas in support of trade, scientific collaboration and national security and law enforcement cooperation**. Globally, we are working with the wider bloc of like-minded, democratic economies which support **greater interoperability of regulatory frameworks on data** and **more stable principles for trusted government access to data**. These areas of work are mutually reinforcing, designed to make the UK the best place for businesses and scientific institutes to undertake data-driven activity. **Our reforms will support the UK's international commitments on the free flow of data.**
>
> Our reforms will mean that **UK scientists are no longer impeded by overcautious, unclear EU-derived rules on how they can use people's personal data**. We will provide scientists with the clarity and confidence they need to get on with life-enhancing and life-saving research. We will simplify the legal requirements around research so scientists can work to their strengths.

Any review of the EU GDPR UK adequacy decision will have to focus on this new Bill, read in the light of these objectives.

Below, I focus on two issues covered by the Bill, comparing the proposed new rules to the ones contained in the EU GDPR, to see if they are "essentially equivalent" to the EU rules – which is the test for adequacy.[5]

3. Selected detailed analyses

3.1 The proposed definition of "personal data" in the Bill and the question of "identifiability" of persons

There have long been issues with the definition of "personal data" in UK law and UK interpretations of that concept, compared to the EU definitions and CJEU interpretations.[6] In 2004, the European Commission commenced infraction procedures against the UK for not fully or properly implementing the 1995 Directive, and one of the many aspects of the 1998 Data Act Protection (introduced to implement that Directive) that the Commission believed did not meet the requirements of the Directive, was the definition of "personal data". In particular, the Directive stated, in Recital 26, that:

> to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller *or by any other person* to identify the said person.

But, as the Commission noted, the 1998 Act did not carry over the Directive's recitals and therefore did not refer to identification by "other persons". In the end, the Commission did not persist with the proceedings. However, there was still little doubt that in this respect UK law fell short of the EU requirements, even while it was still an EU Member State.

Recital 26 to the GDPR (reflecting CJEU case-law) also clarifies that in terms of that instrument, a person is "identified", not just if their identity is known (or deduced), but also if the person can be "singled out" from a larger group of individuals by means of the data (or with additional data) – and this too was never carried over in the UK law.

Admittedly, the answer to the question of when certain data constitute personal data can be difficult, also under the EU GDPR. The text of that same recital 26, for instance, suggests that once data are anonymised, they are completely free for use, because they are no longer personal data and their processing is not subject to the regulation (see the text of the recital, reproduced in the box, overleaf). But that ignores the fact that only too often supposedly anonymised data, when matched with other data, can then allow the re-identification or singling out of the data subject – and there is no doubt that if this is done, if the individual is singled out from an "anonymous" dataset (even if only by reference to a number), the data return to being "personal data" in terms of the EU GDPR.

But such complications aside:[7]

> The ECJ tends to lean towards an expansive definition of personal data. In fact, it appears to expand the concept as necessary to ensure 'a high level of protection of the fundamental rights and freedoms of natural persons' without exceeding the limits required by legal certainty. This approach is seen in judgments such as *Breyer* (paras 31ff), *Scarlet Extended* (para 51), *Nowak* (paras 27ff) and very recently also in *Vyriausioji tarnybinės etikos komisija* (paras 117ff), in which the ECJ was addressing special category data but whose logic can be extended to personal data more generally. As an example, in *Breyer*, the ECJ decided that dynamic IP addresses should be considered personal data, even if the controller is unable to identify the data subject based on the IP address itself (paras 31ff).

So how does the DPDI Bill propose to define "personal data", and how does this differ from the GDPR?

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

The definitions of "personal data", "pseudonymous data" and "anonymous data" in the EU GDPR and in the DPDI Bill

EU GDPR definition **Art. 4(1), with recital 26:**	**DPDI Bill definitions** **Section 3(1), subsections (2) and (3) DPA 2018, with new subsections (3A) and (3B):**[8]
(1) **'[P]ersonal data'** means any information relating to an *identified or identifiable natural person* ('data subject'); an identifiable natural person is one who can be identified, *directly or indirectly*, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **Corresponding recital 26** (edited)**:** To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller *or by another person* to identify the natural person directly or indirectly. Personal data which have undergone **pseudonymisation**, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person [because they still concern an identified or identifiable natural person]. [But T]he principles of data protection should … not apply to **anonymous information**, namely *information which does not relate to an identified or identifiable natural person* or to **personal data rendered anonymous** *in such a manner that the data subject is not or no longer identifiable*. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.	(2) '**Personal data**' means any information relating to an *identified or identifiable living individual* (…). (3) "*Identifiable living individual*" means a living individual who can be identified, *directly or indirectly*, in particular by reference to— (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. *(and see section 3A for provision about when information relates to an identifiable living individual).* *(3A) An individual is identifiable from information "directly" if the individual can be identified without the use of additional information.* *(3B) An individual is identifiable from information "indirectly" if the individual can be identified only with the use of additional information.* **(3A) Information relating to an identifiable living individual** (1) *For the purposes of this Act, information being processed is information relating to an identifiable living individual only in cases described in subsections (2) and (3).* (2) The first case is *where the living individual is identifiable (as described in section 3(3)) by the controller or processor* ***by reasonable means at the time of the processing***. [*continues*]

	(3) The second case is where the controller or processor knows, or ought reasonably to know, that— (a) *another person will, or is likely to, obtain the information as a result of the processing*, and (b) the living individual will be, or is likely to be, *identifiable (as described in section 3(3)) by that person* ***by reasonable means at the time of the processing*****.** (4) *For the purposes of this section, an individual is identifiable by a person "by reasonable means" if the individual is identifiable by the person by any means that the person is reasonably likely to use.* (5) *For the purposes of subsection (4), whether a person is reasonably likely to use a means of identifying an individual is to be determined taking into account, among other things—* *(a) the time, effort and costs involved in identifying the individual by that means, and* *(b) the technology and other resources available to the person.* '**pseudonymisation**' means the processing of personal data in such a manner that it becomes information relating to a living individual who is only indirectly identifiable; but *personal data is only pseudonymised if the additional information needed to identify the individual is kept separately and is subject to technical and organisational measures to ensure that the personal data are not information relating to an identified or directly identifiable living individual.*

(Italics and most emphases in bold added)

At first sight, the main definitions, set out in Article 4(1) EU GDPR and Section 3, subsections (2) and (3) of the Bill – corresponding to the current definitions – are identical (leaving aside the use of the words "living individual" in the Bill where the Regulation uses "natural person").[9] However, the Bill omits one matter that is spelled out in Recital 26 to the GDPR (as noted earlier), contains different rules on another matter, and adds two qualifications, as follows:

- the clarification in Recital 26 to the GDPR that in terms of that instrument, a individual is "identified", not just if their identity is known (or deduced), but also if the individual can be "**singled out**" from a larger group of individuals by means of the data (or with additional data) is not included in the Bill;
- the rules on **identification by "other persons"** (other than the controller or processor) are different and more complex – and more permissive – in the Bill compared to the EU GDPR;
- under the Bill, an individual will only be regarded as "identifiable" – and the data on that individual will therefore only be regarded as "personal data" – if that individual is identifiable by a controller or processor or other person "***by any means that [those persons or entities are] reasonably likely to use***", and the "means reasonably likely to be used" are limited, as noted below; and
- under the Bill, data are only "personal data" if they are identifiable "***at the time of the processing***".

Below, I discuss why each of the above differences will lead to significant differences between the application of the DPDI Bill (if adopted as proposed) and the EU GDPR, and spell out my overall conclusion in this respect.

"Singling out":

Under the **Bill**, a person will only be considered "identified" – and that person's data will only be "personal data" – if that person is individually marked or recorded by reference to "*an identifier such as a name, an identification number, location data or an online identifier, or [to] one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual*". In contrast, under the **EU GDPR** these factors are only given as (typical) examples on a non-exhaustive list ("in particular"): under that instrument, one can also be "identified" – and more in particular, "singled out" – with reference to other factors.

Example: A football club has a set of photos of individuals that it believes were involved in hooliganism, but without any other details of the individuals. A young man is prevented from attending a match because the security guards believe he is one of the suspected hooligans. The guards, acting for the club, have clearly singled that person out – i.e., under the EU GDPR, they have "identified" that person; the photo constitutes personal data; and those data (that photo) must be used in accordance with the EU GDPR. By contrast, under the Bill, if adopted, the guards and the club could argue that they have not identified the person with reference to any of the factors in the closed list (the label "[suspected] hooligan" not being "a factor specific to the identity of [that] individual"); that the data are (the photo is) therefore not personal data; and the use of the photo is not covered by the Bill (or Act once adopted).

Identification by "other persons":

The rule under the EU GDPR is straight-forward. Paraphrased, the second sentence of Recital 26 (the first one quoted in the box on p. 12) makes clear that an individual must be considered identifiable if anyone (the controller, the processor, or any other person) can identify or single out the individual from the data, directly or indirectly, by any "means reasonably likely to be used" by any of those persons.

The text in the bill is much more convoluted, in particular in relation to "other persons". To paraphrase the "second case" of identifiability, set out in proposed new sub-clause (3A)(3): under the Bill (if adopted as proposed), an individual will not be considered identifiable, just because an "other person" (someone else than the controller or processor) can identify that individual by "reasonable means". Rather, that individual will only be regarded as identifiable if the "other person" can identify the individual by such means and the controller or processor also knew (or ought reasonable to have known) that that "other person" would (or was likely to), identify the individual "by reasonable means at the time of the processing". (I am changing the tense from know to knew and from will to would to show more clearly the implication of the rule, as applied in retrospect.)

I will address the issue of "reasonable means" and "at the time of the processing" under the next headings.

Here, I should note that the convoluted "second case" of identifiability set out in the Bill clearly appears to facilitate the making available of de-identified data to "other persons": if a controller passes on de-identified data to an "other person", and does not believe that the "other person" will identify the individuals concerned, the data will, under the Act if adopted as proposed, not constitute "personal data"; the passing on of the data to the "other person" will not constitute "processing of personal data"; and neither the data held by the "other person" nor the processing of those data by that "other person" will be subject to the Act.

"Means reasonably likely to be used":

As it is put in fairly straight-forward language in Recital 26 to the EU GDPR:

> To determine whether a natural person is identifiable, account should be taken of **all the means reasonably likely to be used**, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

The question of what means are "reasonably likely to be used" is, in the EU GDPR, not answered in any rigid way; this is left to the specific context. In a 2007 opinion on the concept of personal data, the Article 29 Working Party (now, under the EU GDPR, replaced by the European Data Protection Board), discussed this as follows:[10]

> ***Means to identify***
>
> Recital 26 of the Directive pays particular attention to the term "identifiable" when it reads that "*whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.*" This means that **a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable"**. If, taking into account "*all the means*

> *likely reasonably to be used by the controller or any other person*", that possibility does not exist or is negligible, the person should not be considered as "identifiable", and the information would not be considered as "personal data". **The criterion of "*all the means likely reasonably to be used either by the controller or by any other person*" should in particular take into account all the factors at stake.** The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, **the interests at stake for the individuals**, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures should all be taken into account. On the other hand, **this test is a dynamic one and should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed.** Identification may not be possible today with all the means likely reasonably to be used today. If the data are intended to be stored for one month, identification may not be anticipated to be possible during the "lifetime" of the information, and they should not be considered as personal data. However, it they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment. The system should be able to adapt to these developments as they happen, and to incorporate then the appropriate technical and organisational measures in due course.
>
> (original italics, emphases in bold and underlinings added)

Although this WP29 opinion, taken under the 1995 Directive, was not endorsed by the EDPB,[11] this can still broadly be taken as the accepted view under the EU GDPR, too. It also chimes with the view of the Court of Justice in *Breyer*, where the Court held the following in relation to the question of whether a dynamic IP address constituted personal data:[12]

> [In that regard], **it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject**.
>
> Thus, as the Advocate General stated essentially in point 68 of his Opinion, **that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant**.
>
> (emphases added)

The crucial point is that in assessing whether, under EU data protection law, in a particular context, certain means that are in principle available to the relevant person or entity are "*likely reasonably to be used*" by that person or entity to identify the individual in question, both the WP29 and the Court take into account, on the one hand, the effort in terms of time, cost and manpower, and, for the WP29, also the advantage that the person who may identify the individual could gain from this identification, and on the other hand, the interests at stake for the individuals, i.e., the risk of harm that identification can entail for that individual.

The Bill qualifies this. It stipulates the following in section 3(1), new sub-section (3A), fourth and fifth paragraph:

(4) For the purposes of this section, an individual is identifiable by a person "by reasonable means" if the individual is identifiable by the person by any means that the person is reasonably likely to use.

(5) For the purposes of subsection (4), whether a person is reasonably likely to use a means of identifying an individual is to be determined taking into account, among other things—

(a) the time, effort and costs involved in identifying the individual by that means, and

(b) the technology and other resources available to the person.

What is notable here is that the relative interests, i.e., the possible advantage that the person who may do the identifying can gain, and the potential harm to the individual who may be identified, are not explicitly mentioned. This ignores the standard spread of harm analysis, according to which, although the probability of a risk may be low, if the potential harm is high, one should still take precautions against it. In simple format:

Likelihood / Consequences	High	Medium	Low
Serious	**High**	**High**	**Medium**
Medium	**High**	**Medium**	**Low**
Not serious	**Medium**	**Low**	**Low**

Wheras the opinion of the WP29 and the *Breyer* judgment of the Court (though also not very explicit in this regard) at least suggest that a risk analysis of this sort is required, the Bill, while perhaps not excluding it, does not appear to suggest such an analysis is needed at all. This means that UK controllers (and processors) are likely to conclude that even if the possible harm to individuals that may result from identification is very serious (e.g., identification of a person at risk from physical attack), the fact that that result is difficult or costly to achieve can be allowed to override that factor.

I would also qualify the Court's suggestion that there is no risk of identification if identification is unlawful. That flies in the face of the facts in the real world, in which highly sensitive information on public figures (and others) is often provided to unauthorised parties (such as journalists) by officials including police officers.

"At the time of the processing":

Finally, the Bill only considers identification "at the time of the processing" of the relevant information. As Chris Pounder has noted in this respect in an insightful blog on this issue (to which I return under the next heading):[13]

Note that "*at the time of the processing*" in the context of "*direct identification*" is likely to be the time the *controller or processor* first obtains the personal data either from the data subject or from another source. The same more or less applies if *indirect identification* is completed by a *controller or a processor* (i.e. data protection obligations kick in as soon as *the additional information* is obtained or is likely to be obtained).

Note also that in the context of "*indirect identification*" and **before** the *additional information* is obtained (or is likely to be obtained), the data processed by a controller or a processor is **not** personal data and is free from data protection obligations.

In the context of "*indirect identification*" by *another person*, the time of the processing is likely to be when the controller or processor knows (or should know) that the "*additional information*" has been obtained (or is likely to be obtained) by that "*another person*" who has expended "*reasonable means*" to identify a data subject.

(original emphases)

This means that (if the DPDI Bill is adopted as proposed) as long as a processor or an "other person" processes (still-)unidentified and (still-)unidentifiable data – i.e., as long as a processor or an "other person" only has de-identified data – the data are not "personal data"; those entities do not process "personal data"; and what they do with the data will therefore not be subject to the law at all. This appears to be irrespective of whether others (notably the controller) has "additional information" available that would allow the (re-)identification of the individuals concerned.

Only if the processor or "other person" were to obtain this or other "additional information" (from the controller or otherwise) that would allow them to link the de-identified data to a specific individual – i.e., to *re-identify* the individual – and if they were to have the means to then do so and were "*reasonably likely*" to use those means (or actually *did* use those means), would the data (again) be regarded as "personal data", and the processing of the data as processing of "personal data", with those entities then – but only then – having to comply with the Act.

In other words, processors or "other persons" who process pseudonymised data are, under the Bill, treated as if they do not process "personal data" at all: the use of such data by such entities – in particular of course entities others than a processor – will be exempt from the law if the Bill is adopted as proposed.

This would appear to be directly contrary to the stipulation in Recital 26 to the EU GDPR that "personal data which have undergone pseudonymisation … should be considered to be information on an identifiable natural person", i.e., to still be "personal data", because they can still be linked to an identifed or identifiable natural person, even if that is by a different person from the one processing the pseudonymised data.

This is a major divergence from the EU GDPR that, if adopted, will have major repercussions, as noted in the Short Note.

Overall conclusion *re* the meaning of "personal data" in the Bill compared to the EU GDPR:

My analysis (like the analyses of others) shows that the re-writing and qualifying of the concept of "personal data" in the DPDI Bill, if adopted as proposed, will significantly affect the overall UK data protection regime. Specifically:

- if an individual is "**singled out**" from a wider group by means other than "*an identifier such as a name, an identification number, location data or an online identifier*", or with reference to "*one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual*", that person is **not** regarded as being "identified"; their data are not regarded as "personal data; and the processing and use of the relevant data will not be subject to the law;
- the Bill clearly appears to facilitate the **making available of de-identified data to "other persons"**: if a controller passes on de-identified data to an "other person", and does not believe that the "other person" will identify the individuals concerned, the data will, under the Act if adopted as proposed, not constitute "personal data"; the passing on of the data to the "other person" will not constitute "processing of personal data"; and neither the data held by the "other person" nor the processing of those data by that "other person" will be subject to the law;
- the Bill, while perhaps not excluding it, does not appear to suggest that a proper risk/harm analysis is needed in relation to possibly re-identifiable data; this means that UK controllers (and processors are likely to conclude that even if the possible harm to individuals that may result from (re-)identification is very serious (e.g., identification of a person at risk from physical attack), the fact that that result is difficult or costly to achieve can be allowed to override that factor;

  and, in direct contradiction to the EU GDPR:

- under the Bill, processors or "other persons" who process **pseudonymised data** are treated as if they do **not** process "personal data" at all: the use of such data by such entities – in particular of course entities others than a processor – will be exempt from the law if the Bill is adopted as proposed.

As Chris Pounder has noted in his blog on this issue:[14]

> The Bill's objective is to widen the scope of [two categories of data: non-personal data and anonymous data] by narrowing the scope of those data that are classified as 'personal data'. That in summary is the name of the game.

In simple terms: the Bill, by re-defining the concept of "personal data" in the ways outlined above, tries to use the UK's "Brexit freedoms" to deviate significantly from EU data protection law and more specifically the EU GDPR, in particular when it comes to the making available and use of de-identified/pseudonymised data.

3.2 The proposed weakening of the lawfulness and purpose-limitation principle

General

The lawfulness and purpose-specification and -limitation purpose (to give it its full name) is one of the foundational principles of data protection, laid down in the earliest international data protection instruments, the 1980 OECD Privacy Principles and the 1981 Council of Europe Convention. Moreover, as the Article 29 Working Party noted:

> The concepts of legal basis and purpose limitation, which were to become the cornerstones of data protection law … started to take shape, and were further developed in the privacy case law of the European Court of Human Rights [under Article 8 of the ECHR]

The EU Charter of Fundamental Rights also stipulates expressly that personal data must be processed for "specified purposes" and that this processing must have a "legitimate basis laid down by law" (Article 8(2) CFR).

Leaving out qualifications in relation to "compatible processing" to which I will come later, the principle is expressed in Article5(1)(b) of the EU GDPR in the same terms as in the 1995 Directive (Article 6(1)(b)), as follows:

> Personal data shall be … collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes …

Lawfulness and legal bases

The requirement that processing of personal data must be for "**legitimate purposes**" is in part linked to the requirement that there be a **legal basis** for the processing (as discussed below), but goes beyond it. As the Article 29 Working Party put it in its 2013 opinion on purpose-limitation, (issued under the 1995 Data Protection Directive that has been succeeded by the EU GDPR, but that is still relevant):[15]

> **[P]urposes must also be legitimate. This notion goes beyond the requirement to have a legal ground for the processing** under Article 7 of the Directive [expanded on in Article 6 GDPR – DK] and also extends to other areas of law. Purpose specification under Article 6 [of the Directive, now Article 5 of the GDPR – DK] and the requirement to have a legal ground under Article 7 [now Article 6 GDPR – DK] are thus two separate and cumulative requirements.
>
> The use of the term 'legitimate' in Article 6 [of the Directive, now Article 5 of the GDPR – DK] provides a link to Article 7 [of the Directive, now Article 6 of the GDPR – DK] [i.e., to the **legal bases** for processing – DK] but also to **broader legal principles of applicable law, such as non-discrimination**. The notion of legitimacy must also be interpreted within the context of the processing, which determines **the 'reasonable expectations' of the data subject**.
>
> (emphases added)

The terms used underline this broad meaning: "legitimate" (F: *licite*; D: *rechtmässig*) is wider than "lawful" (F: *légal*; D: *gesetzmässig*).

The need for a specific and expressly stated ("explicit") **legal basis** was first stipulated in the 1995 Directive, but the details of what can constitute a legal basis were (as suggested by the WP29)[16] greatly expanded on in the EU GDPR (underlining added):[17]

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX [containing "provisions relating to specific processing situations" including research].

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

As noted above, meeting one of the above conditions for processing – i.e., acting on the basis of one of these legal basis – is a necessary, but not a sufficient condition: even if the processing is based on one of these bases, it must still also be "legitimate", e.g., not lead to discrimination.

Moreover, while derogations are possible from the purpose-limitation principle (as noted under the heading "Compatibility", below) and in spite of the language used in the derogation clauses, which only refer to the article containing the lawfulness and purpose-limiation principle (Article 13 in the 1995 Directive; Article 23 in the EU GDPR), **there can be no derogation from the requirement that processing of personal data must serve a "lawful" and "legitimate" purpose: that would be in breach of the fundamental principle of lawfulness in the EU Charter of Fundamental Rights (see Article 52 CFR)**.

The way the DPDI Bill would change the above:

The Explanatory Notes to the Bill say that:[18]

> There is some uncertainty about the different lawful grounds for which private companies can process personal data at the request of public bodies. This can create an unnecessary burden for private organisations and slows down delivery of public services.

So one aim of the Bill is clearly (and explicitly) to make it easier for private companies to "process personal data at the request of public bodies". To this end, Section 5 of the Bill makes the following changes to Article 6(1) of the EU GDPR (new text in italics; main changes also in bold):

Lawfulness and legal bases in the EU GDPR:	**Lawfulness and legal bases in the DPDI Bill:**
1. Processing shall be lawful only if and to the extent that at least one of the following applies: … (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; …	1. Processing shall be lawful only if and to the extent that at least one of the following applies: … (e) processing is necessary for the performance of a task *of the controller* carried out in the public interest or *a task carried out* in the exercise of official authority vested in the controller; ***(ea) processing is necessary for the purposes of a recognised legitimate interest;*** … Point*s (ea) and* (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. … [*continued*]

	5. For the purposes of paragraph 1(ea), processing is necessary for the purposes of a recognised legitimate interest only if it meets a condition in Annex 1.

In simple terms, this means that under the Bill (if adopted), processing of personal data by private entities – and more specifically, disclosure of such data by such entities to public entities – will always be "necessary" and lawful in terms of the law if it meets a condition in Annex 1. Crucially, the main condition set out in that annex is less strict than the ones imposed by the EU GDPR:

In effect, the first paragraph of the Annex stipulates that disclosure of personal data will always be regarded as "necessary for the performance of a task carried out [by a public body] in the public interest" or as "[necessary for] the exercise of official authority vested in the controller" if:

(a) the processing is necessary for the purposes of making a disclosure of personal data to another person in response to a request from the other person, and

(b) the request states that the other person needs the personal data for the purposes of carrying out processing [that is necessary for the performance of a task carried out by a public body in the public interest or in the exercise of official authority vested in the controller and] that has has a legal basis that satisfies Article 6(3) [i.e., is based on a UK law].

Note that the question of whether "*processing is necessary for the purposes of making a disclosure … in response to a request from the other person*" is not the same as the question of whether the disclosure is (or the data are) necessary for the task carried out by the "other person". Rather:

Under this clause, even in its present form, if a UK public body believes it needs certain data from a private entity in order to carry out a statutory function, the private entity has to provide the data, and carry out any processing necessary to comply with the request (e.g., transmitting the data online, or printing it out and sending it in hard copy).

Moreover, the Secretary of State can change any of the conditions in the Annex by means of a statutory instrument (subject to the affirmative parliamentary procedure)[19] if they feel this is "appropriate", taking into account the interests and fundamental rights of the data subjects (DPDI Bill, S. 5(6) and (7)).

<u>This may seem technical, but the effect is massive</u>. In effect, it gives all UK public authorities the right to determine unilaterally what data that are held by private entities – any private entities including e-communications providers, educational, health and financial institutions – they regard as "necessary" for their tasks; and the requested entity must then provide the requested data. The "necessity" test in the EU GDPR is effectively completely emasculated (especially since the supervisory powers of the regulator, the Information Commission, are also weakened, as noted in the Short Note).

Moreover, since private entities established in the EU/EEA that offer goods or services to individuals in the UK will be subject to the UK GDPR, these new duties to provide private sector data to UK authorities on demand will also apply to those EU/EEA-based companies. This could bring them in the invidious position of either being in breach of EU law or UK law.

(Nota Bene: In the above light, other provisions in the Bill are also worrying. For instance, section 64(1) of the Bill stipulates that:

> The Secretary of State or the Treasury may by regulations make provision **requiring a data holder** to publish business data or **to provide business data on request**—
>
> (a) to a customer of the trader, or
>
> (b) **to another person of a specified description (a "third party recipient")**.

The term "**business data**" includes "*information relating to the supply or provision of goods, services and digital content by the trader (such as, for example, information about where they are supplied ...)*" (S. 61(2) under that heading, at (b)). This could include, e.g., in relation to an online service, information about the use of online services or websites, location data, etc.; or offline, details of goods offered, a physical delivery address, etc.. What is more, under section 65(7) of the Bill, the regulations (SIs) can require businesses to use or allow "**specified facilities or services**" to provide the data – which can be read as enabling the mandatory installation of "**back doors**" into business data systems.

This clause is set out in a section of the Bill that appears to be aimed at facilitating the exercise of the right to **data portability**, in particular also in relation to the use of "**smart meters**".[20] However, the wording is sweeping and would appear to allow the Secretary of State to specify that (certain?) "business data" of (a) certain (type of) business be provided (in bulk? through a "back door"?) to a state agency. I am not saying that that is the intention, or that the clause is likely to be used in this way. But there appears to be little to guard against the abuse of this extremely broad power. On UK surveillance powers and practices generally, see section 4 in the Short Note.**)**

<u>Compatability</u>

As noted above, the lawfulness and purpose-limitation principle stipulates that:

> Personal data shall be … collected for specified, explicit and legitimate purposes *and not further processed in a manner that is incompatible with those purposes* …

As noted in a leading commentary on the GDPR:[21]

> This notion of 'compatible' processing of [personal] data has raised numerous questions in practice.

To add some clarification on the issue, Article 6(4) of the EU GDPR (as suggested by the Article 29 Working Party)[22] stipulates that:

> in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
>
> (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

The Article 29 Working Party also stressed that departures from the purpose-limitation principle[23] can only be based on the derogation clause in the EU data protection instrument (at the time, the 1995 Directive; now the EU GDPR), and that this clause imposes limitations on such derogations:[24]

> The limited scope of exceptions confirms that it is not possible to legitimise incompatible processing of personal data simply by relying on one of the grounds listed in Article 7 [of the 1995 Directive; Article 6 EU GDPR – DK]. This is all the more so since the legislative measures adopted under Article 13 of the Directive [Article 23 EU GDPR – DK] must be interpreted restrictively as they are introduced by way of exception to the general principles of Article 6 [of the 1995 Directive; Article 6 EU GDPR – DK]. Therefore, **a legislative measure providing for a legal obligation under Article 7 [of the 1995 Directive; Article 6 EU GDPR – DK] would not necessarily be sufficient to make processing compatible**.

<u>The way the DPDI Bill would change the above</u>:

The Bill, if adopted as proposed, will make the following changes to the main GDPR stipulations relating to compatibility (and then adds further crucial clarification – in fact, exceptions – to the principle, as discussed after this first look at the primary text) (new text in italics; main changes also in bold):

<u>Compatibility in the EU GDPR</u>:	**<u>Compatability in the DPDI Bill</u>:**
Article 5(1)(b): (1) Personal data shall be … … (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes …	**Article 5(1)(b) & (3)**(*amended*)**:** (1) Personal data shall be … … (b) collected *(whether from the data subject or otherwise)* for specified, explicit and legitimate purposes and not further processed *by or on behalf of a controller* in a manner that is incompatible with *the purposes for which the controller collected the data* … … 3. For the avoidance of doubt, processing is not lawful by virtue only of being processing in a manner that is compatible with the purposes for which the personal data was collected." [*continued*]

	[***Article 6(4) is deleted. Instead, a new Article 8A is inserted after Article 8 that includes the following:***]
Article 6(4): Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:	**Article 8A** (*new*)**:** *1. This Article is about the determination, for the purposes of Article 5(1)(b) (purpose limitation), of whether processing of personal data by or on behalf of a controller for a purpose (a "new purpose") other than the purpose for which the controller collected the data ("the original purpose") is processing in a manner compatible with the original purpose.* *2. In making the determination, a person must* take into account, *among other things—*
(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;	(a) any link between the *original purpose* and the *new purpose*;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;	(b) the context in which the personal data *was* collected, *including* the relationship between the data subject and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;	(c) the nature of the personal data, *including whether it is a* special category of personal data (*see Article 9*) or personal data related to criminal convictions and offences (*see Article 10*);
(d) the possible consequences of the intended further processing for data subjects;	(d) the possible consequences of the intended processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	(e) the existence of appropriate safeguards (*for example*, encryption or pseudonymisation).
	[*continued*]

	*3. **Processing of personal data for a new purpose is to be treated as processing in a manner compatible with the original purpose where—*** *(a) the data subject consents to the processing of personal data for the new purpose and the new purpose is specified, explicit and legitimate,* *(b) the processing is carried out in accordance with Article 84B [for research etc. purposes: see the text]—* *(c) the processing is carried out for the purposes of ensuring that processing of personal data complies with Article 5(1) [lawfulness] or demonstrating that it does so,* *(d) **the processing meets a condition in Annex 2**, or* *(e) the processing is necessary to safeguard an objective listed in Article 23(1)(c) to (j) and is authorised by an enactment or rule of law.*

The crucial change is in the new Article 8A, para. (3)(d) that says that any secondary processing that meets a condition in the new Annex 2 (that is not in the EU GDPR) must always be regarded as "compatible" with the original purpose.

In effect, the main condition in this new Annex 2 is the same as the main one set out in Annex 1, discussed above under the heading "*Lawfulness and legal bases*". It covers **disclosures of personal data by a private entity to a public entity for a purpose described in Article 6(1)(e), i.e., for the performance of a task of the controller [read here: the receiving poblic entity] carried out in the public interest or for a task carried out in the exercise of official authority vested in the controller [*idem*]**.

The first paragraph of Annex 2 says, in effect, that such disclosures are always to be regarded as "compatible" with the original purpose for which the data were processed by the private sector provider of the data if:

a. the processing is necessary for the purposes of making a disclosure of personal data to another person in response to a request from the other person, [and]

b. the request states that the other person needs the personal data for the purposes of carrying out processing that—

(i) is described in Article 6(1)(e) [i.e., that the requesting public body needs the personal data for one of the above-mentioned purposes],

(ii) has a legal basis that satisfies Article 6(3) [i.e., that there is a law or subsidiary instrument that authorises the obtaining of the data by the public body], and

(iii) is necessary to safeguard an objective listed in Article 23(1)(c) to (j) [i.e., is necessary to safeguard a major public interest].

To again put this in simple terms, it follows from the first condition in Annex 2 that under the Bill (if adopted), disclosures of personal data by private entities to public entities will always be regarded as "compatible" with the original purposes for which the data were processed by the private entities.

This is again clearly incompatible with the EU GDPR

The other conditions set out in Annex 2 are somewhat more in accordance with the EU GDPR in that they specify that a disclosure of personal data are only "compatible" with the original purpose for which they were obtained if the disclosure is "necessary" for the secondary aims mentioned in those other conditions: *public security*, *detecting, investigating or preventing crime*, *collecting taxes etc.*, to meet a *legal obligation or court order*, protecting the *vital interests of a person*, or *safeguarding vulnerable individuals*, dealing with *emergencies*.

However, the other conditions set out in Annex 2 fail to stipulate (as the EU GDPR does in Article 23) that the processing for those purposes – *in casu*, the disclosures for such secondary purposes – must also "respect the essence of the fundamental rights and freedoms [of the data subjects]" and must not only be "necessary" but also "proportionate" to the secondary aim that is being pursued. And those additional stipulations in the EU GDPR – missing from the DPDI Bill – of course reflect the fundamental rule of law requirements set out in Article 52 of the EU Charter of Fundamental Rights.

The omissions of these requirements again constitute a significant departure from the EU standards.

- o – O – o –

Prof. Douwe Korff
Cambridge (UK), 27 October 2022

(Notes overleaf)

NOTES:

[1] Data Protection and Digital Information Bill – Explanatory Notes, 18 July 2022, *Legal background – Data Protection*, paras. 53 - 61 (p. 18), available at:
https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf

[2] See: https://bills.parliament.uk/bills/3322. Note however that this is mainly in the form of a series of amendments to the UK Data Protection Act 2018 and the UK GDPR. The government has as yet not released a consolidated version of the (extremely complex) UK data protection laws with the proposed DPDI Bill amendments.

[3] See:
https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments
(emphases added)

[4] Government's response to its *Data: A new direction* consultation (footnote 8, above), *Introduction*.

[5] CJEU, *Schrems I* judgment, para. 73.

[6] In 2003, the UK Court of Appeal held, with reference to the CJEU judgment in *Lindquist*, that the term "personal data" as used in the then applicable law, the Data Protection Act 1984, only covered personal information whose content was focused on a particular individual who was the subject of personal data, and touched on privacy-related matters: *Durant v Financial Services Authority*, [2003] EWCA Civ 1746; [2004] FSR 28, available at:
https://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf
(In that case, the court also held that paper-based personal information was subject to the law only if the information was recorded in a very highly structured filing system.)
The successor to the 1984 Act, the Data Protection Act 1998 (adopted to implement the 1995 Data Protection Directive) used essentially the same definition of "personal data".
However, subsequent judicial and non-judicial guidance has brought the application of the term in this respect closer to the "expansive" approach of the CJEU, noted in the quote on p. 10 of this note. See:
https://www.pinsentmasons.com/out-law/news/meaning-of-personal-data-should-not-be-derived-solely-from-durant-case-says-high-court-judge
That issue is therefore left aside in this note.

[7] Tiago Cabral and Sophia Hassel, *T-384/20 OC v European Commission: The General Court Falls out of Line on Personal Data*, European Law Blog, 17 October 2022, available at:
https://europeanlawblog.eu/2022/10/17/t-384-20-oc-v-european-commission-the-general-court-falls-out-of-line-on-personal-data/#more-8599
Note that In a judgment of 4 May 2022, the General Court appears to move away from this "expansive" approach – which is what caused the authors to write the above blog – but as they rightly note, the case has been appealed to the full Court and it is highly unlikely that that will follow this clear departure from the jurisprudence. See:
EU General Court, *OC v. European Commission* (Case No. T-384/20), 4 May 2022, ECLI:EU:T:2022:273, available at:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=258784&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=1875369
Yet another case, in which the Court is asked whether a bank's log data constitute personal data, *Pankki S* (Case No. C-579/21), is pending.

[8] The numbering of the articles in the DPDI Bill will be streamlined in the final Act and are likely to differ from the Bill as currently drafted.

[9] In this attachment, I will generally refer to the person to whom data relate as an "**individual**", and to those who may process the data as "**persons**" (or entities). This avoids confusion in some contexts. The individual to whom data relate becomes a "**data subject**" if the individual is identified or can be identified from the data – but quite a bit of my note addresses precisely the question of when this can be said to happen, i.e., when the "individual" becomes a "data subject" – and is then protected by data protection law.

[10] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP136), adopted on 20 June 2007, available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

[11] Cf. European Data Protection Board, Endorsement 1/2018 [of various WP29 guidelines and opinions], adopted on 25 May 2018 (the day on which the EU GDPR entered into application), available at:
https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf

[12] CJEU judgment of 19 October 2016 in *Breyer v. Federal Republic of Germany* (Case C-582/14), ECLI:EU:C:2016:779, paras. 45 – 46, available at:
https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

[13] Chris Pounder on his *Amberhawk* blog, *New Data Protection Bill defines "personal data" below DPA1984 threshold*, 4 August 2022, available at:
https://amberhawk.typepad.com/amberhawk/2022/08/new-data-protection-bill-defines-personal-data-below-dpa1984-threshold.html

[14] *Idem*.

[15] Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP203), adopted on 2 April 2013, section II.2.1, *First building block: purpose-specification*, at p. 12, available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[16] *Idem*, Executive Summary, at p. 3.

[17] Article 7 of the Directive contains 186 words; Article 6 of the EU GDPR 671, with Article 7 (204 words) further expanding on one legal basis, consent, and Article 8 (177 words) expanding yet further on "conditions applicable to child's consent in relation to information society services", adding between them another 381 words, making 1052 in all – a more than five-fold increase in detail.

[18] Explanatory Notes (note 1, above), para. 11

[19] See section 3 in Attachment 1.

[20] *Idem*, sections on *Smart Data Scheme*, paras. 37 – 40 and 49 – 52.

[21] Christopher Kuner *at al*., The EU General Data Protection Regulation (GDPR): A Commentary, OUP, 2020, *Commentary on Article 5*, p. 315. See there for a more detailed discussion.

[22] Article 29 Working Party, Opinion 03/2013 on purpose limitation (note 15, above), *Executive Summary*, p. 3. The factors that are to be taken into account, listed in Article 6(4) EU GDPR, quoted in the text, directly draw on the WP29 opinion (*idem*). That clause replaces one proposed by the Commission that was strongly criticised by the WP 29: see pp. 36 – 37 of the opinion.

[23] As noted under the previous heading, there can be no derogations from the "lawfulness" principle.

[24] Article 29 Working Party, Opinion 03/2013 on purpose limitation (note 15, above), section III.3, *Excveptions under Article 13 of the Directive*, pp. 37 – 38, emphases added.

- o – O – o -