Douwe Korff

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

UPDATE ON THE

Opinion on
the future of personal data transfers
from the EU/EEA to Israel & the Occupied Territories

This document contains an update on my opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories of 4 February 2021. The update relates in particular to proposed amendments to the Israeli Privacy Protection Act, introduced in the Israeli Parliament, the Knesset, in the autumn of 2021, and currently in preparation for second and third readings.

Cambridge, UK

23 February 2022 (final)

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

UPDATE ON THE
Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories

About this opinion:

This update, like the original opinion,* was commissioned by the European Middle East Project, EuMEP:
https://eumep.org/

Also like the original opinion, the update seeks to contribute to the discussions about the implications of the EU's policy of "differentiation" between Israel and the Occupied Territories, based on international law, for the future of personal data flows between the EU and Israel and the OTs, and to the review of the 2011 EU Commission Adequacy Decision on Israel under the EU General Data Protection Regulation (GDPR) that is currently underway.

* For links to the original opinion and the executive summary of that opinion, see footnote 1, below.

About the author:

Douwe Korff is a Dutch comparative and international lawyer specialising in human rights and data protection. He is emeritus professor of international law at London Metropolitan University and visiting professor at the universities of Zagreb and Rijeka in Croatia; an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin.

After extensive rule of law work in Central Asia, the Caucasus and the Balkans for the OSCE, the Council of Europe and the European Union, for the last twenty years he has focussed on digital rights including data protection. In that field, he has done many studies for the EU, the Council of Europe, the UN (ITU), the British Commonwealth, and the UK authorities. Douwe Korff works closely with civil society and digital rights groups including Privacy International, Statewatch, European Digital Rights (EDRi), the Foundation for Information Policy Research, etc. He gave expert evidence on the implications of the U.S. surveillance activities revealed by Edward Snowdon to inquiries by the Council of Europe, the EU and the German Bundestag.

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

UPDATE ON THE
Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories

CONTENTS:

- o – o – o –

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

UPDATE ON THE
Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories

Executive Summary

On the issue of adequacy of the Israeli PPA and the proposed amendments to the PPA:

It cannot be said that the Israeli Privacy Protection Act (PPA), even if amended as proposed in the 14th Amendment Bill, will provide "essentially equivalent" protection to the GDPR **in substantive terms**. At the very least, the changes that are apparently envisaged in a future 15th Amendment Bill will have to be adopted before the legal situation in Israel can be said to come close to the one in the EU. But of course, one would have to see those future further changes in detail before any firm conclusions about adequacy after their adoption could be drawn.

It can also not be said that the PPA, even if amended as proposed in the 14th Amendment Bill, will provide "essentially equivalent" protection to the GDPR **in procedural/enforcement terms**.

Even if all the proposed changes under the 14th Amendment Bill to the PPA were to be adopted, Israeli law will continue to be glaringly deficient **in relation to access to EU data by the Israeli law enforcement and national security agencies** (an issue further highlighted in the current NSO/Pegasus scandal). For that reason alone, it should be considered impossible for the European Commission to issue a new positive adequacy decision on Israel at present. Only fundamental changes to the Israeli security laws, to bring them in line with the European Essential Guarantees for surveillance (EEGs), could remedy this.

In sum: Even if amended as proposed in Bill No. 14, the Israeli PPA will still manifestly fail to meet the GDPR standards in terms of substance, procedure, enforcement, and (especially) undue access to data by the Israeli security and intelligence agencies.

On the issues of territoriality (*which are not addressed in the proposed amendments*):

As I already concluded in my opinion in this regard:

Israel cannot be granted a new positive EU adequacy decision and then enjoy free personal data exchanges with the EU unless it starts treating onward transfers of data from Israel to the Occupied Territories (OTs) as transfers abroad, at least as concerns EU data.

If Israel were to be granted a new adequacy decision without this change, that would perpetuate the current situation, which is the data protection equivalent of allowing goods from the settlements to be labelled as "*Made in Israel*" or of allowing settlement entities to benefit from EU funding programmes.

It may be hoped that the European Commission can persuade the Israeli authorities to address the issues of territoriality in the potential 15th Amendment Bill.

In sum: For any new adequacy decision, Israel would have to adopt changes to the substantive provisions of the PPA that go beyond those envisaged in the 14th Amendment Bill (but that may be included in the putative 15th Bill); make changes to the status of the Data Protection Commissioner; bring its security laws in line with the EEGs; and treat transfers of personal data from Israel proper to the OTs as onward transfers. Until then, no new adequacy decision can be issued: that would be in breach of the GDPR and of the EU's "differentiation" policy.

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

UPDATE ON THE
Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories

1. Introduction

1.1 The original opinion

As explained in the original opinion and in the executive summary of the original opinion,[1] that opinion sought to contribute to discussions about the future of personal data flows between the European Union (EU) and the European Economic Area (EEA)[2] on the one hand and Israel and the Occupied Territories (OTs) on the other. In that context, it also sought to contribute to the review of the 2011 EU Adequacy Decision on Israel that has allowed for free flows of personal data between the EU/EEA and Israel (but only Israel proper, within its 1967 borders) since then.[3] The 2011 adequacy decision on Israel was adopted under the then-applicable 1995 Data Protection Directive. It must be reviewed under the EU General Data Protection Regulation (GDPR) that came into application in May 2018 and significantly tightened EU data protection law.[4] The review is currently under way.

More specifically, the opinion addressed the question of how the EU's policy of "differentiation" between Israel and the OTs, which has been affirmed by rulings of the Court of Justice of the EU (CJEU), is and should be applied in the EU's treatment of flows of personal data to Israel and to the OTs. This issue should be seen as an important aspect of the review of the EU adequacy decision on Israel.

As also explained in the original opinion, the reason to focus on Israel and the OTs was threefold. Firstly, transfers of EU personal data to this region pose special challenges in the light of international law and this "differentiation" policy. Secondly, there were serious doubts about the appropriateness of the 2011 EU positive "adequacy" decision on Israel, even at the time; and there are more serious doubts about the "adequacy" of Israeli privacy law in the light of the GDPR.

---

[1] Available at:
https://www.ianbrown.tech/wp-content/uploads/2021/07/KORFF-Opinion-EU-Israel-data-transfers-final.pdf
(full text; hereafter "**Opinion**")
https://www.ianbrown.tech/wp-content/uploads/2021/07/KORFF-Exec-Summ-EU-Israel-data-transfers-final.pdf
(executive summary; hereafter "**the executive summary**")

[2] The European Economic Area comprises the 27 EU Member States and Iceland, Liechtenstein and Norway. EU data protection law applies to all EU and EEA states, hence the references in the text to "EU/EEA".

[3] Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332), Commission Document 2011/61/EU, OJ L 27, 1.2.2011, p. 39–42, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, available at:
https://eur-lex.europa.eu/eli/reg/2016/679/oj
The need for adequacy assessments of the privacy or data protection laws of non-EU/EEA countries (so-called "third countries") as a basis for permitting free flows of personal data to such countries is addressed in Chapter IV of the GDPR: see the opinion, section 3.2, *EU Adequacy decisions and requirements for onward transfers*.

Third, Israel and the OTs warrant scrutiny because of Israel's extensive surveillance activities that raise questions about potential access by Israeli state security agencies to EU citizens' data. The July 2020 *Schrems II* judgment of the CJEU invalidated EU arrangements for data flows to the United States precisely because of such concerns – with clear implications in relation to other third countries including Israel.[5] My opinion explained in some detail:

- **the inadequacy of Israeli privacy law in relation to EU data protection law** in terms of substance,
- **the inadequacy of Israeli privacy law in relation to EU data protection law** in terms of procedural/enforcement requirements, and
- **the inadequacy of Israeli privacy law in relation to EU data protection law** in terms of protection of EU data from undue access by Israeli authorities (i.e., in relation to Israeli surveillance law and practices);[6]
- the issue of Israeli settlements in the Occupied Territories (OTs) and **the EU's so-called policy of differentiation** which distinguishes between activities of Israel within its pre-1967 borders and its activities beyond the Green Line;[7] and (related to this)
- **issues of territoriality**, i.e., the conflict between the Israeli approach to the territorial application of the Israeli Privacy Protection Act and the EU policy of differentiation.[8]

As summarised in the executive summary, **the opinion concluded that**:[9]

- **the current (unamended) Israeli Privacy Protection Act (PPA) manifestly fails to meet the now-applicable GDPR standards in terms of substance, procedure, enforcement, and undue access to data by the Israeli security and intelligence agencies;**
- **the Israeli approach to the issues of territorial application of the PPA and transfers of personal data to East Jerusalem, the Golan Heights and the Israeli settlements in the West Bank is <u>fundamentally incompatible</u> with the EU views on the territorial scope of EU-Israel relations in general, and with the stipulations in that regard in the 2011 Adequacy Decision on Israel in particular;**
- **unlike in other areas of EU-Israel relations, the territorial limitations in the EU Adequacy Decision have not been enforced in practice; and it appears that the EU has so far quietly tolerated Israel's non-compliance with these provisions.**
- ***The current situation is the data protection equivalent of allowing goods from the settlements to be labelled as "Made in Israel" or of allowing settlement entities to benefit from EU funding programmes.***

---

5 CJEU Grand Chamber judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), ECLI:EU:C:2020:559. See section 2.4, below.

6 Opinion, section 4; executive summary, section 3.

7 Opinion, section 2; executive summary, section 2.

8 Opinion, section 5; executive summary, section 4.

9 Opinion, sections 4.3, 5.3 and 6.3; executive summary, section 5.

1.2 The proposed amendments to the Israeli Privacy Protection Act

In the autumn of 2021, the Israeli Ministry of Justice issued a proposal for amendments to the 1981 Privacy Protection Act, with an explanatory memorandum.[10] The proposal was approved by the Knesset Ministerial Committee for Legislation for the first reading on 7 November. It was discussed in the plenary on 24 January 2022 and is now in preparation for second and third readings in the Knesset Constitution, Law and Justice Committee.[11]

The proposals are known as "**Bill No. 14**" (or "**Amendment 14**"). As briefly summarised by Dan Or-Hof, a member of the Protection of Privacy Council established under the PPA:[12]

> What follows are the essence of Bill No. 14's proposed changes:
>
> • **An update to definitions** to adapt terms to the modern era and align them, in part, with GDPR terms, such as: "data protection commissioner" instead of "databases registrar," "database controller" instead of "database owner," and GDPR-like definitions to "data" (the equivalent to "personal data" under the GDPR) and "data with special sensitivity."
>
> Additionally, the bill introduces new definitions such as "biometric identifier" and "processing," which includes "collection" and "use" of data.
>
> **We note** that the authors of the bill at the Justice Department offered only a partial alignment with GDPR definitions. Specifically, the bill does not remove the outdated reference to "databases" (as opposed to "data"), presumably to avoid additional considerable changes in the law.
>
> • **New criminal offenses**: up to three years imprisonment for misleading a DPC supervisor or for receiving personal data fraudulently. These offenses join the already-existing criminal offenses under the current law, which include up to five years of imprisonment for wilful confidentiality violations.
>
> ...
>
> • **New administrative fines of up to NIS 3,200,000 (about USD $1 million)** for violations associated with a database of more than 1 million sensitive data records, and an additional NIS 64,000 (about USD $20,000) per day for continuous or repetitive violations.

---

[10] *The Ministerial Committee for Legislation approved the Minister of Justice's proposal to advance the amendments In the Privacy Protection Law*, 7 November 2021, available at: https://www.gov.il/he/departments/news/amendments_privacy_protection_act (in Hebrew only)
There is to date no official or otherwise authoritative English translation of the proposed amendments or the explanatory memorandum. This Update was written on the basis of Google Translate translations of the texts and of summaries and outlines provided by law firms' websites.

[11] Knesset page on the Privacy Protection Bill (Amendment No. 14), 5722-2022, available at: https://main.knesset.gov.il/Activity/Legislation/laws/Pages/LawBill.aspx?t=lawsuggestionssearch&lawitemid=2167975 (in Hebrew only)

[12] Dan Or-Hof, *Summary of proposed new law* for the International Association of Privacy Professionals (IAPP), 26 January 2022, available at: https://iapp.org/news/a/a-turning-point-for-privacy-laws-in-israel/ (original emphases in bold; some commentary ["We note"] omitted or reduced, indicated by "..."; "Omissions" heading added) (Hereafter: "**the IAPP Overview**")

Processing data for non-consented purposes and unauthorized use of data constitute the most severe violations.

Additionally, the bill sets a price tag of up to NIS 320,000 (about USD $100,000) per violation of a provision under the 2017 Protection of Privacy Regulations (Data Security). Accordingly, the accumulated risk can go up to several USD millions. The DPC will have the authority to replace fines with a warning or a commitment to avoid further violations.

We note the proposed fines are significantly higher than the fines under the existing law, but are also significantly lower than the maximum fines under the GDPR. ...

- **Far-reaching investigatory powers**, including the authority, without a court order, to have a person identify themselves to a DPC supervisor, demand information, documents and computer data from every person, and access non-residential premises where a database is used.

We note that the new powers are similar to police powers, while lacking commensurate judicial due process, and further lack sufficient constraints on DPC powers to prevent "function creep" and ensure these powers are not used in an unproportionate manner.

- **Appointment of data protection officers in law enforcement and national security agencies**, who will report to the DPC. The DPOs ("privacy supervisors," as referred to in the bill) will be appointed to one term of up to seven years. They will have the same investigatory powers as DPC supervisors have, but they will be subordinated to either the head of the agency or to a senior official who reports directly to the head of the agency.

The DPC will instruct the DPOs on professional matters and the DPOs are prohibited from assuming conflicting positions. The agency must provide the DPO with the "proper means" necessary for the DPO to function. The bill also sets out a job description that includes preparing an annual compliance plan and reports, review of the agency's procedures and policies, handling complaints, preparing reports to the DPC, and training of personnel.

We note that the Protection of Privacy Council (disclosure: the author is a member of the council) has time and again advised the Justice Department to include a statutory obligation to appoint DPOs, in alignment with modern privacy legislation. The explanatory words accompanying the bill do not explain why only security agencies will need to appoint DPOs.

- **A considerable reduction of mandatory database registrations.** Fifteen years after a special committee produced the Shofman Report recommending reducing the duty to register databases with the databases registrar, Bill No. 14 will likely realize this recommendation.

The amended law will still require registration subject to specific criteria. These include the number of records (data on more than 500,000 individuals); sensitivity (data on more than 100,000 individuals will require a report to the DPC); collection method (data on more than 100,000 individuals that was not collected from them); and type of organization or activity (public entities and data brokers).

We note that the reduction of database registrations is meant to eliminate unwarranted bureaucracy while providing the DPC with the ability to focus on a limited number of high-risk databases. However, given the proposed thresholds under Bill No. 14, the number of

registrations would be still considerably high, thereby failing to properly support the two purposes of this amendment.

- **A special arrangement for violations during elections.** The head of the Central Elections Committee must grant the DPC specific permission to impose a fine on or use its other enforcement powers against a political party during election time. Permission will be granted unless the DPC enforcement power will considerably harm the violating party's election efforts and the public interest associated with the elections will outweigh the importance of the DPC's administrative activities.

We note that this is a counterintuitive and potentially damaging arrangement. The DPC should have independent powers to stop a political party from gaining unethical and unlawful advantage during election time via violating individuals' privacy. Such independence is not an obstacle, but rather crucial for proper democratic elections processes.

Omissions:

The bill lacks substantial provisions related, among other things, to enhancing data subject rights, expanding the lawful grounds of processing, appointing DPOs, requiring impact assessment procedures, and legislating the privacy-by-design and by-default principle.

The Justice Department publicly stated it intends to follow Bill No. 14 with Bill No. 15 to address these matters.

Dramatic increase in data security and purposeful processing risks

According to the Protection of Privacy Authority 2019 and 2020 report to the Knesset (the Israeli Parliament), 54% of enforcement actions — 105 out of 195 — were focused on data security violations, particularly violations of 2017 DSR provisions, with an additional 35% addressing violations of the purposeful processing obligation. Nearly 90% of enforcement activities, therefore, were focused on these two areas.

Under current law, the Protection of Privacy Authority does not have the authority to impose fines on data security violations. Similarly, the current law empowers the authority with very limited power to impose fines (up to about USD $8,000 per violation) on data use for non-consented purposes.

Bill No. 14 will change this risk dramatically, offering the DPC the authority to impose a USD $1 million fine for unauthorized use of data and for violating the purposeful processing principle [known in the EU as the purpose limitation principle – DK], alongside up to USD $100,000 for every violation of a provision under the 2017 DSR. These may include violations of obligations related to access management, encryption, communication security, security audits, penetration tests, updates of IT systems and much more.

The bill will also provide the DPC with broad court order-free access to data and computer systems, thereby removing a judicial scrutiny barrier from the investigatory process.

It is reasonable to assume the DPC will continue its enforcement focus on data security and purposeful processing violations, but with much more power in its hands.

Key takeaways

The current main risk associated with privacy violations in Israel comes from class actions. This risk is on the rise because the number of privacy actions is rising.

Bill No. 14 will increase administrative and criminal risk substantially. Companies that do business in Israel should focus their compliance efforts first and foremost on cybersecurity measures and procedures in compliance with the 2017 DSR, on providing proper disclosures and on securing informed consent to the processing of the data.

1.3 The aim of the update

After a brief introduction (sub-section 2.1), section 2 of this update revisits the main issues noted above, at 1.1:

- the question of substantive adequacy of Israeli privacy law (in terms of the EU GDPR) (sub-section 2.2);
- the question of procedural/enforcement adequacy of Israeli privacy law (in those terms) (sub-section 2.3);
- the issue of access to transferred data by Israeli authorities (sub-section 2.4); and
- the issues of territoriality and onward transfers (sub-section 2.5).

Each issue is reviewed to assess if the conclusions set out in the box on p. 6, above, need to be revised in the light of the proposed amendments to the PPA. As may already be clear from the overview of the proposed amendments in the previous sub-section, not all of these issues are actually addressed in the proposed amendments.

My findings and conclusions are summarised in an Executive Summary (set out at the beginning of this paper for easy reference).

- o – O – o –

2. The issues revisited

2.1 Introduction

My original opinion noted that in 2011 the European Commission felt that, on the basis of the opinion of the Article 29 Working Party (WP29) that was established under the then-applicable 1995 Data Protection Directive (now replaced under the GDPR by the European Data Protection Board), it could issue a positive adequacy decision on Israel because (in the WP29's view) the Israeli rules were roughly similar to those in the 1995 Directive, and because the WP29 and the Commission believed that the Israel rules would over time become closer to the EU rules.[13] However, as explained in my opinion, now, under the GDPR, much stricter tests are applied, as underlined by the case-law of the Court of Justice of the EU (CJEU).

Specifically, under the GDPR, in order for a third country – i.e., *in casu*, Israel – to be held to provide "adequate" protection to personal data, it must be able to show that it provides "essentially equivalent" protection to the GDPR in all respects: substantive and procedural, and with regard to access to data transferred to the third country from the EU by the third country's authorities (including its intelligence and law enforcement agencies). The third country law must also prevent transfers of personal data sent to the third country from the EU/EEA to another country or territory in relation to which the EU has not issued an adequacy decision (so-called "onward transfers").[14] In relation to Israel, the latter issue is seriously complicated by the different views on territoriality adopted by the EU and Israel.[15]

The sub-sections below look at the same issues as were addressed in my opinion and examine whether the proposed amendments would redress the deficiencies noted in the opinion.

2.2 Substantive protection

In my opinion, I found the PPA to be **glaringly defective** compared to the GDPR in terms of the substantive protection it provides. Indeed, I concluded that even in 2011 the Commission should not have issued its positive adequacy decision on Israel because it did not even provide "adequate" protection to personal data compared to the then-applicable 1995 Data Protection Directive.[16]

The proposed amendments to the PPA do address a number of those glaring deficiencies. In particular, the definition of the term "**information**" in the PPA is to be brought closer to the definition of "**personal data**" in the DPR; it is to be:

---

[13] Opinion, section 4.1, *Inadequacy of the 2011 Adequacy Decision under the 1995 Data Protection Directive*, sub-section 4.1.1, Introduction.

[14] For details, see again the opinion, section 3.2, *EU Adequacy decisions and requirements for onward transfers*.

[15] *Idem*, section 5, *Issues of territoriality*. The mutually incompatible views on territoriality are illustrated in charts on pp. 63, 65 and 68 – 69 of the Opinion that are replicated in sub-section 2.5, below.

[16] *Idem*, sub-section 4.1.2, Substantive protection.

> data relating to an identified or identifiable person, directly or indirectly, by reasonable means, including IDs, biometric information, and any other unique identifying data.

The term "**database owner**" is also brought close to the GDPR definition of "**controller**"; it is to be:

> a person who determines, alone or together with another, the purposes of processing the information in the database, or a body authorized by law to manage a database.

And, as under the GDPR, biometric and genetic data, data about a person's race or [ethnic] origin and data about a person's physical or mental health are to be considered "**sensitive information**", as will "information about the privacy of a person's personal life, including the conduct and conduct of the individual", which presumably includes information about "a natural person's sex life or sexual orientation" (which are the words used in the GDPR).

The proposal also stresses the central importance of the **purpose-limitation principle** (referred to in the proposal as the **principle of closeness of purpose**) and if adopted would make it a general criminal offence to breach this principle (rather than limiting it effectively to registered databases and supervision by the PPC).

Adoption of those changes would however not really make the PPA "essentially equivalent" to the GDPR in substantive terms.

First of all, the Act will continue to effectively apply only to information processed by automated means ("by digital means"). At the very least, any new adequacy decision would therefore still (like the 2011 one) have to exclude manual data.

Second, whether the new or revised terms will actually be applied in essentially the same way as the corresponding terms in the GDPR is far from certain. For instance, as noted above, the proposed new definition of "[personal] information" expressly refers to identifiability "by reasonable means". This can be said to be in line with the clarification of that issue in Recital 26 to the GDPR that says that:

> [t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used ...

However, the recital then goes on to add considerable detail, by giving as an example:

> singling out, *either by the controller or by another person* to identify the natural person directly or indirectly.

To this it adds:

> To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

In the EU, the term "personal data" is consequently interpreted very broadly. It includes, for instance, pseudonymised data that may be reidentified by a third party that holds additional data.[17] Whether the term "[personal] information" in the proposed amendment, if adopted, will be equally broadly interpreted and applied in Israel is unsure (although the proposal for the amendments lists and quotes a number of court cases that do suggest a broad interpretation).

The proposed amendments also do not really introduce **the general principles of proportionality and necessity** into the PPA. In relation to public sector controllers (database owners), such principles may well be applied under relevant public or administrative law in Israel. But whether those same tests will be applied to private sector controllers (as they are in the EU) is less clear.

The proposed amendments also do not address **the general issue of legal bases for processing** that is of core importance to the GDPR. On the only main legal basis for processing that is mentioned in the PPA, **consent**, the proposed amendments do not address the fact that the PPA expressly allows for processing on the basis of *implied* consent, whereas under the GDPR, for consent to be valid, it has to be "unambiguously indicated" and, in relation to sensitive data, "explicit". In this respect, the PPA would clearly still not be "essentially equivalent" to the GDPR, even if all the currently proposed amendments were to be adopted (on possible future further amendments, see below).

The most crucial issue however relates to the absence from the proposals of the **principles of accountability** (Art. 5(2) GDPR) and **data protection by design and default** (Art. 25). The accountability principle was newly explicitly introduced in the GDPR to compensate for the abolition of the registration (notification) system for personal data processing operations under the 1995 Data Protection Directive. It has major implications in terms of requiring controllers (and processors) to be able to "demonstrate compliance" with the GDPR principles (and indeed, with all the GDPR obligations). It follows from this principle that controllers must keep detailed records of all their processing operations, with details of the legal basis for each operation, the data used, disclosures, retention periods, etc. – as further elaborated on in Article 30 GDPR. Those records should "demonstrate" that all their processing is indeed GDPR compliant "by design and default" – and they must be made available to the data protection supervisory authorities on request (Art. 30(4)).

Also important in that regard are the new requirements under the GDPR for all controllers in the public sector and many controllers in the private sector to appoint a **data protection officer** (DPO) (Section 4, Arts. 37 – 39 GDPR) and for controllers to carry out a **data protection impact assessment** (DPIA) in relation to processing operations that pose risks to the rights and interests of data subjects (Art. 35).

Neither the PPA in its present form nor the proposed amendments envisage anything that could be regarded as "essentially equivalent" to these GDPR requirements. The task of the "security

[17] Cf. WP29 Opinion 05/2014 on Anonymisation Techniques (WP216), adopted on 10 April 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

supervisor" that must already be appointed in certain cases (PPA, S. 17B(a)) is limited to ensuring information security (S. 17B(b)), while mandatory appointment of data protection officers (referred to in the Bill as "privacy supervisors") is limited to law enforcement and national security agencies (even though the Protection of Privacy Council "has time and again advised the Justice Department to include a statutory obligation to appoint DPOs, in alignment with modern privacy legislation" [such as the EU GDPR]).[18] There is no provision requiring DPIAs in the PPA as it stands, and none are proposed in the Bill.

Provisions on legal bases, privacy/data protection by design and default, the appointment of DPOs more generally, and DPIAs are supposed to be added later, in a 15th Amendment Bill.[19] However, under the Adequacy Referential that applies under the GDPR, the European Commission cannot adopt a positive adequacy decision on Israel merely on the basis that it hopes and expects these issues to be addressed at some stage in the future. (As I pointed out in the opinion, the Commission was in fact already wrong to adopt the 2011 decision on that basis).

In my view, it cannot be said that the PPA, even if amended as proposed in the 14th Amendment Bill, will provide "essentially equivalent" protection to the GDPR in substantive terms. At the very least, the changes that are apparently envisaged in a future 15th Amendment Bill will have to be adopted before the legal situation in Israel can be said to come close to the one in the EU. But of course, one would have to see those future further changes in detail before any firm conclusions about adequacy after their adoption could be drawn.

2.3 Procedural/enforcement adequacy[20]

I noted in my opinion that protection under the PPA was (and is) effectively limited to personal data in registrable databases – and that many databases (in particular, databases containing information on less than 10,000 people) need not be registered. Under the proposed Bill, the registration requirement is to be greatly reduced:

> The proposed amendment significantly reduces the obligation to register but does not eliminate it. ... It is ... proposed that the registration obligation apply to large databases, which have **over 100,000 data subjects**, and in addition have **special sensitivity** due to the type of information contained therein (***sensitive data***) or due to the type of database owner (***public body***) or due to the purpose of the processing of the information (collection of information for the purpose of [***data brokering***] or due to the manner in which the information is collected in the database (i.e., when ***the information was not collected from the data subjects or with their consent***).
>
> (Explanatory Memorandum to the Bill, emphases added)

Note that these conditions are cumulative.

---

18 IAPP overview (footnote 12, above).

19 *Idem*.

20 Opinion, section 4.1.3, *"Procedural/enforcement" guarantees (independent supervision)*.

Removing the registration (notification) requirement is sensible and in line with what was done in the EU, where the 1995 Data Protection Directive had such a scheme but this was left out of the GDPR: registration as a means of ensuring compliance never worked. As the proposal for the amendments to the PPA put it:

> Professional experience over the years shows that the obligation to register at its current scope is not a significant tool in the hands of the Registrar. In addition, a common mistake is that the registration of the database constitutes a "kosher certificate" to the processing activity performed. The majority opinion in the Schoffman report recommended reducing the obligation to register, and ... a memorandum of law on the subject was circulated in 2012. The registration fee for databases was abolished in 2017.

However, under the GDPR the abolition of the registration (notification) scheme was compensated by the introduction of the principles of accountability and data protection by design and default, the mandatory appointment in many cases of DPOs, and the mandatory carrying out of DPIAs in relation to "risky" processing (as noted in the previous sub-section).

The proposed amendments provide considerably less compensation for the abolition of the registration duty. As also noted in the previous sub-section, the proposed amendments would make compliance with the purpose limitation principle a more general requirement. And **the supervisory authority is to be given extensive new powers**:[21]

> Under current law, the Protection of Privacy Authority does not have the authority to impose fines on data security violations. Similarly, the current law empowers the authority with very limited power to impose fines (up to about USD $8,000 per violation) on data use for non-consented purposes.
>
> Bill No. 14 will change this risk dramatically, offering the DPC the authority to impose a USD $1 million fine for unauthorized use of data and for violating the purposeful processing principle, alongside up to USD $100,000 for every violation of a provision under the 2017 DSR. These may include violations of obligations related to access management, encryption, communication security, security audits, penetration tests, updates of IT systems and much more.
>
> The bill will also provide the DPC with broad court order-free access to data and computer systems, thereby removing a judicial scrutiny barrier from the investigatory process.
>
> It is reasonable to assume the DPC will continue its enforcement focus on data security and purposeful processing violations, but with much more power in its hands.

While these are clearly significant improvements in terms of supervision and enforcement, they do not suffice to make the system "essentially equivalent" to the GDPR in procedural/enforcement terms.

Crucially, as noted in the original opinion, the criteria that were applied in the WP29 opinion that underpinned the 2011 adequacy decision did not yet require that the data protection/privacy

---

21 IAPP overview (footnote 12, above).

supervisory authority in a third country be **independent**, but this is now required under the GDPR. The 2009 WP29 opinion rather generously concluded that, under the rather lax standards of the time, the Israeli supervisory agencies had:[22]

> an adequate degree of independence for the purposes that are established for supervisory authorities regulated by the Directive.

However, as also noted in the opinion, the requirements relating to supervisory authorities under the GDPR are much stricter and much more elaborate than under the then-applicable 1995 Data Protection Directive, in particular in relation to their independence.[23] Those stricter requirements are also applied in practice within the EU: following earlier cases concerning questions about the independence of supervisory authorities in Germany and elsewhere, in November 2021, the European Commission launched formal proceedings against Belgium, alleging that the country's data protection authority is not independent.[24] The EU authorities are now also taking a much closer look at the status and powers of third country's data protection supervisory authorities.[25]

Unfortunately, the proposed amendments to the PPA do not address this issue at all: the Database Registrar is to be renamed "Data Protection Commissioner" (although the name of the law is not changed to Data Protection Act), but his independence is not enhanced.

In my view, it can also not be said that the PPA, even if amended as proposed in the 14th Amendment Bill, will provide "essentially equivalent" protection to the GDPR in procedural/enforcement terms. Perhaps this – in particular, the status and independence of the Data Protection Commissioner – can be addressed in a future 15th Amendment Bill, but there are no specific indications to that effect as yet.

This brings me to the third issue that needs to be addressed in any assessment of the adequacy of privacy/data protection law in a third country: the question of access to personal data that may be transferred to the third country by state agencies of that third country.

---

[22] Article 29 Working Party, Opinion 6/2009 on the level of protection of personal data in Israel (WP165), adopted on 1 December 2009, p. 14, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf

[23] See in particular Article 52 GDPR.

[24] The Brussels Times, *European Commission questions independence of Belgium's Data Protection Authority*, 13 November 2021, available at: https://www.brusselstimes.com/news/belgium-all-news/193520/european-commission-questions-independence-of-belgiums-data-protection-authority

[25] Cf. the detailed analysis of the Japanese PPC in the most recent adequacy decision, on Japan (the first adequacy decision issued since the coming into application of the GDPR: Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, paras. 95 – 102, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC

2.4 Access to transferred data by Israeli authorities[26]

As noted in the opinion, the issue of access by Israeli authorities to data transferred from the EU/EEA to Israel was **not addressed at all in the 2009 WP29 opinion or in the 2011 European Commission adequacy decision on Israel**.

However, as also noted there, this issue has become important in relation to adequacy assessments: Article 45(2) GDPR expressly requires that the Commission, when assessing the adequacy of the level of protection in a third country, must "*in particular, take account of" (inter alia) "relevant legislation … including concerning … national security … and the access of public authorities to personal data*" (under such laws), as well as "*the existence and effective functioning of one or more independent supervisory authorities in the third country … with responsibility for ensuring and enforcing compliance with the data protection rules*."

More specifically, the excessive access that US authorities can gain to such data under US surveillance laws and the absence of appropriate judicial remedies against this undue access were two of the main reasons why, in its *Schrems II* judgment, the Court of Justice of the EU invalidated the adequacy decision on the USA that rested on the so-called "Privacy Shield".[27]

The Court made clear that (in line with general principles of EU law) access to data transferred to a third country – and interception of data in transit to a third country – by the third country's agencies must be based on clear, precise and publicly accessible legal rules ("**law**"); must serve a "**legitimate aim**" (which of course includes law enforcement and national security); must be limited to what is (strictly) "**necessary**" and "**proportionate**" to that aim; and must be subject to appropriate – i.e., in principle, **judicial – review**, to which the persons affected can have access.[28]

In my opinion, I discussed Israeli surveillance in some detail,[29] and established that:

- The Israeli security agencies, in particular SIGINT Unit 8200, have highly advanced surveillance capabilities, similar to those of the US's NSA and the UK's GCHQ;[30]
- Israeli surveillance in the OPT is manifestly incompatible with general international, but also especially specifically European and EU fundamental rights standards, and also

---

[26] Opinion, section 3.2.2, *Requirements for a positive adequacy decision*, sub-section ii., Access to EU data by a third country's intelligence agencies.

[27] See footnote 5, above. For a detailed discussion of the GDPR requirements and of this case (and other CJEU case-law), see: Ian Brown and Douwe Korff, Exchanges of personal data after the Schrems II judgment, study carried out at the request of the European Parliament's Civil Liberties (LIBE) Committee into the future of EU – US flows of personal data, July 2021, available at:
https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf
See in particular section 2.3.1.3, *Requirements relating to access to personal data by state authorities* (p. 34ff.) and more in particular the write-up under the heading "*CJEU requirements relating to indirect or direct access to personal data by third country intelligence agencies*" (p. 43ff.).

[28] *Schrems II* (footnote 5, above), paras. 174 – 176, quoted in the Brown/Korff study (previous footnote), at p. 45.

[29] Opinion, section 4.2.4*, Inadequate protection against indiscriminate surveillance*.

[30] *Idem*, sub-section ii, Israeli surveillance capabilities and practices.

covered mobile and online communications between individuals in the EU and entities and individuals in the OPT, which are all routed through Israel proper;[31] and that:

- Even within Israel proper:[32]
  - The various Israeli intelligence agencies have extremely wide powers of surveillance and access to data including e-communications data, not only in the OPT but also in Israel proper (and thus also East Jerusalem and the Golan Heights), also through mandatory (but secret) "back doors" into the providers' systems and/or by means of spyware or zero-day exploits, with very limited procedural or substantive safeguards;
  - Those powers allow for the indiscriminate, untargeted, bulk collection of data;
  - There is no truly independent supervision over the use of these powers; and
  - There are no effective, independent remedies available to individual data subjects (either Israeli or non-Israeli) whose data may be, or may have been, accessed by the agencies.

I concluded that:

> The above findings are all in stark contrast to the ruling in the CJEU's *Schrems II* judgment that a third country cannot be held to provide "adequate" "essentially equivalent" protection to personal data if its intelligence agencies can gain "generalised and indiscriminate" access to data transferred to the third country from the EU, and/or if there are no effective, independent remedies against undue access. The Court has further clarified in its *PI* and *LQDN* judgments that the EU Charter of Fundamental Rights requires that access by intelligence agencies must be based on a publicly available law that on its face sets out clear and strict limitations on access to such data.

The only way in which the proposed amendments to the PPA touch on the issue of surveillance is that (as noted earlier) they provide for the appointment of DPOs in the law enforcement and national security agencies. However, those proposals do not change the agencies' (from the EU point of view, excessive) powers or the (from the EU point of view, excessively lax) rules covering the use of these powers, or the lack of serious avenues of redress.

Even if all the proposed amendments to the PPA were to be adopted, Israeli law therefore will continue to be glaringly deficient in relation to access to EU data by the Israeli law enforcement and national security agencies. For that reason alone, it should be considered impossible for the European Commission to issue a new positive adequacy decision on Israel at present. Only fundamental changes to the Israeli security laws, to bring them in line with the European Essential Guarantees for surveillance, could remedy this.

---

31 *Idem*, sub-section iii, Surveillance in the Occupied Palestinian Territory.

32 *Idem*, sub-section iv, Surveillance in Israel proper.

A final note on this issue:

In my opinion, I already noted that concerns had been raised about the use and possible abuse of the Israeli state's surveillance powers in relation to the Corona virus pandemic.

More recently, a large public scandal erupted in Israel around reports that Israeli police used the controversial *Pegasus* spyware developed by the Israeli tech company NSO to spy on politicians and activists:[33]

> Israel police uses NSO's Pegasus spyware to remotely hack phones of Israeli citizens, control them and extract information from them ... Among those who had their phones broken into by police are mayors, leaders of political protests against former Prime Minister Benjamin Netanyahu, former governmental employees, and a person close to a senior politician. Calcalist learned that the hacking wasn't done under court supervision, and police didn't request a search or bugging warrant to conduct the surveillance. There is also no supervision on the data being collected, the way police use it, and how it distributes it to other investigative agencies, like the Israel Securities Authority and the Tax Authority.

A day later, the same source reported that:[34]

> The police's cyber division employs external hackers to collect intelligence on targets. The hackers don't have security clearance, were not trained as police officers, and are exposed to [i.e., gained access to – DK] extremely private and secret information

These scandals underline the glaring deficiencies summarized earlier in this section and in my view affirm the impossibility on the part of the European Commission to issue another positive adequacy decision on Israel right now.

It is possible that these scandals will lead to wider, and more critical debate on state surveillance in Israel (and the OTs), and perhaps even to changes in the laws and practices to bring them in line with international (and European) standards on surveillance, as set out in the European Essential Guarantees on surveillance,[35] discussed in my opinion.

That would make it more likely that a new positive adequacy decision could be issued on Israel – but of course, that would depend on any such actual progress (and it would still not resolve the territoriality/differentiation issues discussed in the next section).

---

[33] Calcalist, *Israel police uses NSO's Pegasus to spy on citizens*, *CTECH*, 18 January 2022, available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html
On general concerns about *Pegasus*, see, e.g., *EU to launch rare inquiry into Pegasus spyware scandal*, *Guardian*, 10 February 2022, available at: https://www.theguardian.com/news/2022/feb/10/eu-close-to-launching-committee-of-inquiry-into-pegasus-spyware?CMP=Share_iOSApp_Other

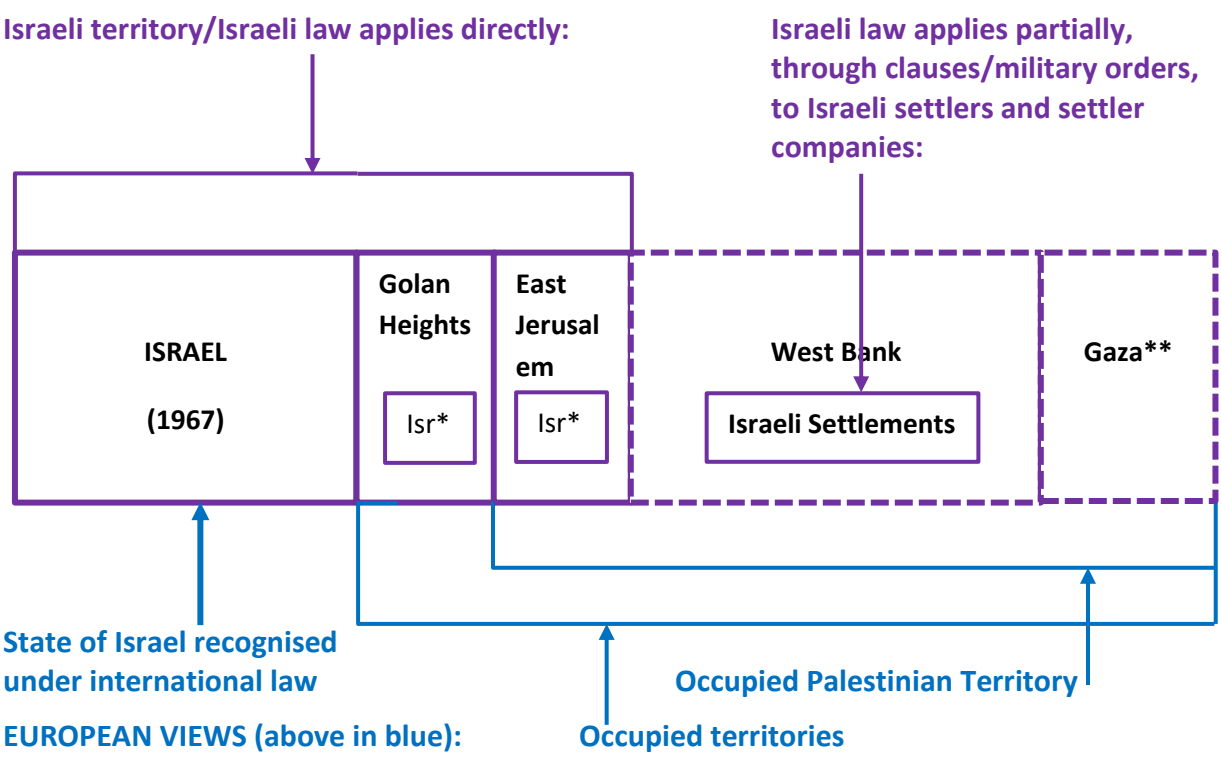
[34] Calcalist, *Move over NSO: Israeli police is paying private hackers to spy on citizens*, *CTECH*, 19 January 2022, available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3927495,00.html

[35] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

2.5 Territoriality and onward transfers

In my opinion, I discussed at some length the EU policy of "differentiation" between Israel proper (Israel within its 1967 borders) and the Occupied Territories (OTs), including East Jerusalem and the Golan Hights,[36] as well as the different views on "territoriality" adopted by Israel on the one hand and the EU on the other.[37] In particular, I noted that Israel views East Jerusalem and the Golan Heights as part of its national territory to which its national laws apply in the same way as they do within Israel proper, and that Israel also increasingly extends the application of those national laws to West Bank settlements.[38] And I discussed the way this worked out in relation to the PPA.[39] I illustrated these different views in the following charts:

Chart 1: Incompatible views on territoriality



Notes:

* There are also Israeli settlements in East Jerusalem and the Golan Heights where (as explained in the text), Israeli law applies directly, as it does in Israel proper (i.e., Israel within its 1967, internationally recognised borders).

** Gaza is considered by most of the international community as occupied territory (part of the OPT), despite Israel's claim that it no longer occupies the territory (in which there are no longer Israeli settlements).

---

36 Opinion, section 2.2, *EU differentiation policy and CJEU case-law*.

37 *Idem*, section 5, Issues of territoriality.

38 *Idem*, sub-section 5.1.1, Territorial application of Israeli law generally.

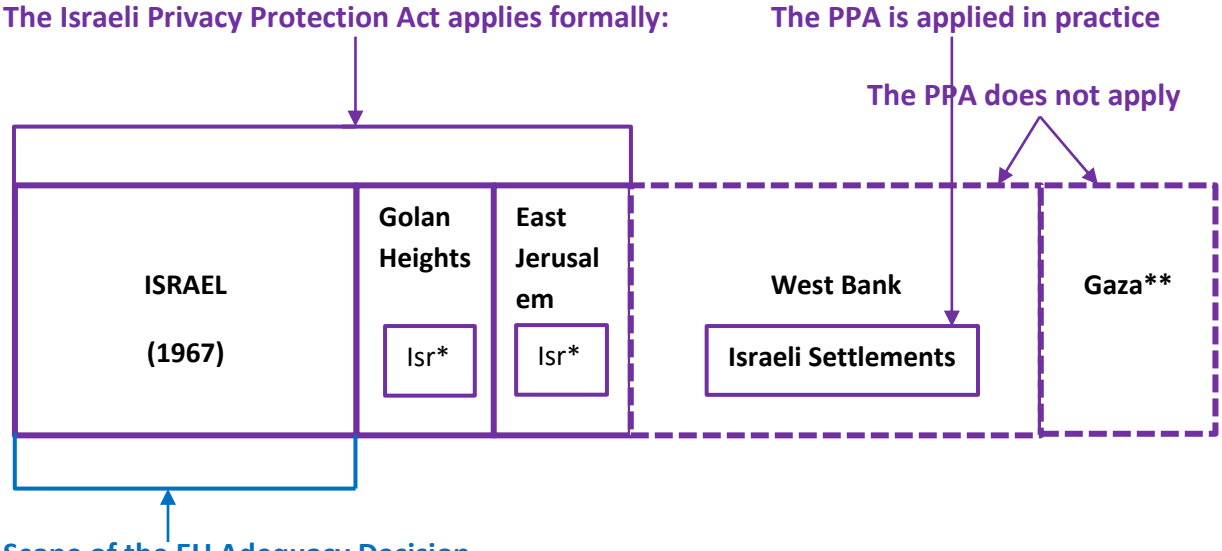
39 *Idem*, sub-section 5.1.2, Territorial application of the PPA.

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

UPDATE ON THE
Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories

Chart 2: The territorial application of the PPA

ISRAELI VIEWS (below in purple):



EUROPEAN VIEWS (above in blue)

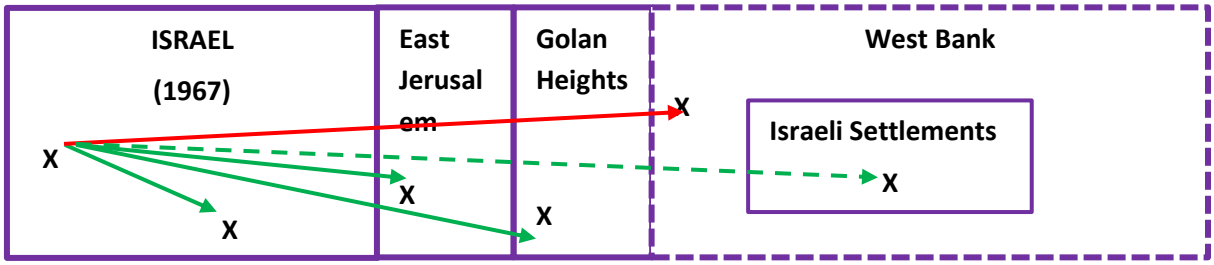
Chart 3: Incompatible views on transfers ("X" = company)

I. ISRAELI VIEW:

→ = internal domestic disclosure

→ = transfer abroad ("onward transfer" if EU/EEA data)

- - → = in practice treated as an internal domestic disclosure



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

UPDATE ON THE
Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories

I concluded that (as I put it in the executive summary of my opinion):

> The Israeli approach to the issues of territorial application of the PPA and transfers of personal data to East Jerusalem, the Golan Heights and the Israeli settlements in the West Bank is fundamentally incompatible with the EU views on the territorial scope of EU-Israel relations in general, and with the stipulations in that regard in the 2011 Adequacy Decision on Israel in particular;
>
> Unlike in other areas of EU-Israel relations, the territorial limitations in the EU Adequacy Decision have not been enforced in practice; it appears that the EU has so far quietly tolerated Israel's non-compliance with these provisions; and that:
>
> *The current situation is the data protection equivalent of allowing goods from the settlements to be labelled as "Made in Israel" or of allowing settlement entities to benefit from EU funding programmes.*

The first point to be made in this update is that **the proposed amendments to the PPA in Bill No. 14 do not address this issue at all**. Indeed, it would appear likely that even the putative Bill No. 15 (that is so far only promised but has not yet been written, let alone submitted to the Knesset) may not address this issue.

The second point is that **in the review of the 2011 adequacy decision that is currently under way, this can no longer be ignored**: if the European Commission were to adopt a new positive adequacy decision on Israel without addressing this (in more detail, with clearer implications), than was done in the – never enforced – territorial stipulation in the 2011 decision, that would not only be in direct contravention of the (since 2011, strongly reinforced and CJEU-endorsed) policy of "differentiation", but also go directly against the GDPR stipulations on onward transfers.

There is perhaps a glimmer of hope in this regard, which is the putative Amendment Bill No. 15: since it is only in *statu nascendi* (or perhaps even just a glimmer in the eye of the Ministry of Justice) it may be hoped that the European Commission can persuade the Israeli authorities to address the issues of territoriality in relation to privacy/data protection law in that Bill.

Specifically, as concluded in my original opinion, the European Commission should make it clear that (even leaving the other issues of adequacy noted earlier aside), no new adequacy decision can be issued unless and until Israel starts treating transfers of personal data from Israel proper to the OTs as "onward transfers" in terms of the GDPR.

My findings and conclusions are summarised in an Executive Summary (set out at the beginning of this paper for easy reference).