# Douwe Korff

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


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

Cambridge, UK

4 February 2021

(Final version)

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

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

**About this opinion:**

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

It 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.

It also seeks to contribute to the review of the 2011 EU Commission Adequacy Decision on Israel under the EU General Data Protection Regulation (GDPR) that is currently underway.

**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*

**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*

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

# Executive Summary

## 1. Why this opinion on transfers to Israel and the OTs is submitted now

The opinion seeks to contribute to discussions about the future of personal data flows between the European Union on one hand and Israel and the Occupied Territories (OTs) on the other. In that context, it seeks to contribute to the review of the 2011 EU Adequacy Decision on Israel under the EU General Data Protection Regulation (GDPR) that is currently underway.

The reason to focus on Israel and the OTs is twofold. Firstly, transfers of EU personal data to this region pose special challenges in the light of international law and 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). Secondly, they 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.

## 2. Israeli settlements in the OTs in international and EU law

In line with international law including UN Security Council and General Assembly resolutions, the EU has never recognized Israel's sovereignty over the occupied territories and considers Israeli settlements in the occupied territories to be "illegal under international law".

Over time, this position has been progressively translated into the EU's legal and administrative practice, thus giving rise to **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.

The principle of territorial differentiation has been applied to a number of aspects of EU-Israel relations including trade, EU funding, product certification, consumer labelling and other areas.

The EU's differentiation policy has been validated by CJEU judgments (*Brita* 2010, *Psagot* 2019, and Western Sahara rulings of 2016 and 2018).

This opinion addresses the question of how this policy 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 data transfers to Israel.

## 3. The inadequacy of Israeli privacy law in terms of EU data protection law

Under EU data protection law, personal data may only be freely transferred to a non-EU/EEA[1] country (a so-called "third country") if the European Commission has issued an Adequacy Decision confirming that the country in question provides "adequate" protection to such data.

The tests for adequacy have been significantly tightened since the coming into application of the GDPR in 2018. The CJEU has held that the law in the third country must provide "essentially

[1] EU data protection law also applies to the three non-EU Member States of the European Economic Area (EEA), Iceland, Liechtenstein and Norway, hence the occasional references in the text to "EU/EEA" and "non-EU/EEA" countries.

equivalent" protection to EU data protection law. Furthermore, "onward transfers" of personal data from that third country to another non-EU/EEA country may not "undermine" the protection accorded by EU law. And the authorities in t7he third country may not give their domestic authorities – in particular, their intelligence agencies – excessive, undue access to the data.

In 2011, the European Commission issued an Adequacy Decision for Israel, based on an assessment that the 1981 Israeli Privacy Protection Act 5741-1981, as amended in 2007 ("PPA"), provided "adequate" protection in terms of the then applicable EU data protection instrument, the 1995 EC Data Protection Directive. However, as the Opinion shows, this decision was fundamentally flawed, even then, in terms of the then-applicable standards.

Since then, the EU standards have been very significantly tightened, while the Israeli Privacy Protection Act has changed little, if at all.

**The Opinion shows that the Israeli Privacy Protection Act 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.**

## 4. Issues of territoriality

In line with general EU policy, the 2011 Adequacy Decision on Israel stipulates that it only applies to Israel within its internationally-recognised 1967 borders. In EU data protection terms, all transfers of EU personal data from Israel to any country or territory outside those borders constitute "onward transfers" for which special safeguards must be adopted.

However, the Israeli PPA applies in the Golan Heights and East Jerusalem, which have been annexed by Israel, in the same way as it does in Israel proper and there are no restrictions on transfers of personal data from Israel proper to these areas. Moreover, in practice, for the purposes of the PPA, individuals and companies in the settlements in the West Bank are also treated in the same way as individuals and companies in Israel proper, East Jerusalem and the Golan Heights.

**In other words: 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.**[2]

**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 quietly tolerates 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.***

[2] These mutually incompatible views are illustrated in charts on pp. 63, 65 and 68 – 69 of the Opinion.

## 5. Conclusion

In theory, the EU has three options: a) to allow the 2011 Adequacy Decision on Israel to continue; b) to issue a new Adequacy Decision; or c) to repeal or suspend the 2011 decision without replacing it (for now).

**It follows from my analyses that the only option that is compatible with the standards set by the CJEU in recent judgments in both the areas of data protection and in relation to territorial differentiation, is the last one: to withdraw or suspend the 2011 Adequacy Decision.**

**Subsequently, the EU can try and persuade Israel to bring its data protection law and practice in line with EU standards and territorial requirements, and to end indiscriminate mass surveillance, to allow the EU to issue a new Adequacy Decision in the future.**

**Specifically with regard to territorial differentiation, the EU would have to obtain Israel's agreement to oblige Israeli data controllers and processors to treat onward transfers of EU/EEA personal data to the OTs as "transfers of personal data abroad" and not as internal domestic disclosures.**

- o – o – o -

Douwe Korff (Prof.)
Cambridge (UK), 5 February 2021

# 1. Introduction

## 1.1 Why this opinion on transfers to Israel and the OTs is submitted now

This opinion seeks to contribute to the discussions about the implications of the European Union's policy of "differentiation" between Israel and the Occupied Territories, based on international law (discussed in section 2.1, below), for the future of personal data flows between the EU and Israel and the OTs. In that context, it also seeks to contribute to the review of the 2011 EU Commission Adequacy Decision on Israel under the EU General Data Protection Regulation (GDPR) that is currently underway.*

*NOTE: "Adequacy decisions" are decisions of the European Commission recognizing that a non-EU country (in EU terminology, a "third country") gives "adequate" protection to personal data. If it does, personal data may be freely sent to that country (subject to requirements in relation to "onward transfers" to yet other countries); without an adequacy decision, the EU rules impose strict conditions on such transfers. Israel is one of a dozen non-EU countries that have received an adequacy decision from the EU. In reaching its decision, the European Commission must take into account the opinion of the European Data Protection Board (EDPB) that is made up of representatives of the data protection supervisory authorities of all the EU Member States and the EU's own European Data Protection Supervisor. The decision must also be approved by the "Article 93 Committee", made up of representatives of the EU Member States' governments. It is also scrutinized by the European Parliament.

It is apposite to provide this opinion now, in the beginning of 2021, because the EU is in the process of (somewhat belatedly) reviewing all the "adequacy" decisions for third countries in the light of the new, stricter rules on transfers of personal data to such countries under the GDPR that came into application in 2018, compared to the less demanding and less detailed rules in the GDPR's predecessor, the 1995 EC Directive on Data Protection, under which all but one of those decisions, including the 2011 Adequacy Decision on Israel, were taken (cf. Article 97 GDPR). The review must also take into account several judgments of the Court of Justice of the EU (CJEU), including *Schrems I* and *II*, *Privacy International* and *La Quadrature du Net*, that significantly further tighten the tests for "adequacy", including by clarifying that a third country may only be held to provide "adequate protection" to personal data if it effectively provides "essentially equivalent" protection to such data as is ensured within the EU by the GDPR, and if EU data are protected from undue indiscriminate access to the data by the third country's agencies.

The reason to focus on Israel and the Occupied Territories is twofold. Firstly, transfers of EU personal data to those areas pose special challenges in the light of international law and the EU's territorial "differentiation" policy, which has been affirmed by CJEU rulings. Secondly, they 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.

## 1.2 Overview

After this introductory part, part two of my opinion will discuss the status of the Israeli settlements in the West Bank from the point of view of public international law, with reference to relevant UN Security Council and General Assembly resolutions and the advisory opinion of the International Court of Justice on the construction of a wall in the Occupied Palestinian Territory, and outline 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.

Part three provides a brief introduction to EU data protection law, before focusing on the issue central to the opinion: the requirements of the EU General Data Protection Regulation (GDPR) on transfers of personal data from the EU to non-EU countries (so-called "third countries") and specifically the rule that personal data may only be freely transferred to third countries that have been held to provide "adequate" protection to such data – a requirement that the Court of Justice of the EU has held to mean that the relevant third country must provide "essentially equivalent" protection to personal data to what is provided within the EU by the GDPR. More specifically, in this part I discuss the checklist provided in that regard by the European Data Protection Board (EDPB) – it's so-called "Adequacy Referential".

In part four, I note first of all that the European Commission's 2011 positive adequacy decision on Israel was itself flawed: the 1981 Israeli Privacy Protection Act did not even meet the then-applicable (and much less demanding) criteria for data protection adequacy. I then show that the PPA (which has changed very little since 2011) certainly does not meet the CJEU/EDPB current standards elucidated under the GDPR, not in terms of substance, nor in terms of procedural/enforcement matters, and in particular not because of the undue access that the Israeli security and intelligence agencies have to any data transferred from the EU to Israel proper (or to the Occupied Territories).

Part five addresses special issues of importance to the EU "differentiation policy": the questions of the territorial application of Israeli law generally and of the PPA specifically, and the issue of personal data transferred from the EU to Israel proper being further, "onwardly" transferred to the Occupied Territories.

I summarise my findings in part six, where I then discuss the implications (in three different scenarios), and draw my conclusions.

- o – O – o –

# 2. Israeli settlements in the Occupied Territories in international and EU law

## 2.1 The Israeli settlements in public international law

Relevant **UN Security Council** and **General Assembly** resolutions make clear that Israeli settlements in the Occupied Territories cannot be considered as part of the State of Israel and that these settlements violate international law. Already in 1979, UNSCR 446 stated:[3]

> The establishment by Israel of settlements in the Palestinian territory occupied since 1967, including East Jerusalem, has **no legal validity** and constitutes **a flagrant violation under international law**. (emphasis added)

In the most recent UNSCR on the issue, resolution 2334 from 2016, the Security Council reaffirms this and underlines that:[4]

> it will not recognize any changes to the 4 June 1967 lines, including with regard to Jerusalem, other than those agreed by the parties through negotiations.

Further, it calls upon all states to:

> **distinguish, in their relevant dealings, between the territory of the State of Israel and the territories occupied since 1967**. (emphasis added)

In its advisory opinion on the legal consequences of the construction of a wall in the Occupied Palestinian Territory of 9 July 2004, the **International Court of Justice** also held, in unambiguous terms that:[5]

> **the Israeli settlements in the Occupied Palestinian Territories (including East Jerusalem) have been established in breach of international law.** (emphasis added)

## 2.2 EU differentiation policy and CJEU case-law

The EU has never recognized Israel's sovereignty over the occupied territories and has been explicit about its non-recognition since at least 1998.[6] As stated, for example, in the European Commission's 2015 guidelines on the origin indication of Israeli settlement products:[7]

---

[3] UNSCR 446 (1979), quoted in subsequent resolutions 452 (1979), 465 (1980), 605 (1987), 1544 (2004) and 2334 (2016); UNGA Resolution 74/88 (2019) and many previous ones.

[4] UN SCR 2334, adopted on 23 December 2016, para. 1, available at: https://www.un.org/webcast/pdfs/SRES2334-2016.pdf

[5] International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004, para. 120, available at: https://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf

[6] European Commission, Implementation of the interim agreement on trade and trade-related matters between the European Community and Israel, 12 May 1998, available at: http://aei.pitt.edu/3345/1/3345.pdf
See in particular Section III, on pp. 7 – 8, which neatly sums up the position in international law and the EU view.

[7] European Commission, Interpretative Notice on indication of origin of goods from the territories occupied by Israel since June 1967, 12 November 2015, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC1112(01)&from=EN

> The European Union, in line with international law, **does not recognise Israel's sovereignty over the territories occupied by Israel since June 1967**, namely the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem, and **does not consider them to be part of Israel's territory**, **irrespective of their legal status under domestic Israeli law**. The Union has made it clear that it will not recognise any changes to pre-1967 borders, other than those agreed by the parties to the Middle East Peace Process (MEPP). (emphasis added)

The EU also considers Israeli settlements in the occupied territories to be "illegal under international law"[8], in accordance with the above-mentioned advisory opinion of the International Court of Justice and UNSC resolutions.

Over time, this position has been progressively translated into the EU's legal and administrative practice, thus giving rise to **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.[9]

This was expressed in the EU Foreign Affairs Council Conclusions on the Middle East Peace Process, adopted in 2012, as follows:[10]

- The EU expresses its commitment to ensure that – in line with international law – **all agreements between the State of Israel and the EU must unequivocally and explicitly indicate their inapplicability to the territories occupied by Israel in 1967.**

In 2017, the EU has further stated:[11]

- **The EU will continue to distinguish, in its relevant dealings, between the territory of the State of Israel and the territories occupied since 1967.**

The principle of territorial differentiation has been applied to a number of aspects of EU-Israel relations:

- **Trade**: Products from Israeli settlements are excluded from preferential treatment under the EU-Israel Association Agreement. This has been operationalised through the so-called

---

[8] See e.g. Statement by the High Representative Josep Borrell on Israeli settlement announcements, 22 February 2020, available at: https://eeas.europa.eu/headquarters/headquarters-homepage/75037/statement-high-representative-josep-borrell-israeli-settlement-announcements_en

[9] For details, see Hugh Lovatt and Mattia Toaldo, EU Differentiation an Israeli Settlements, European Council on Foreign Relations Policy Brief, 2015, available at: https://www.ecfr.eu/page/-/EuDifferentiation-final3.pdf

[10] Council of the European Union, Council conclusions on the Middle East Peace Process, Brussels, 10 December 2012, point 4, available at: https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/134140.pdf
Emphasis added. This is repeated in subsequent FAC Conclusions on MEPP.

[11] Statement by Mr. Vale de Almeida on behalf of the EU and its Member States at the United Nations Security Council Open Debate on the Middle East, including the Palestinian Question, 20 April 2017, emphasis added, available at: https://unispal.un.org/DPA/DPR/unispal.nsf/0/EBB3B64AA27C128F8525810D006B2755

Technical Arrangement agreed between the EU and Israel in 2004. Israel has to ensure that the postal code of the place of production appears on the documentation for exported goods enabling the EU customs to identify the settlement products and deny preferential treatment.[12]

- **EU funding**: In 2013, the European Commission issued guidelines preventing EU grants and loans from benefitting Israeli entities and activities in the occupied territories.[13] In order to participate in EU funding programmes such as the research cooperation programme Horizon 2020, Israel agreed to abide by the guidelines. Israeli applicants for participation in such EU programmes must sign a declaration confirming their compliance with the EU guidelines.
- **Product certification**: Since 2014, the EU has refused to recognize Israeli certificates for organic products and for products of animal origin from Israeli settlements. With regard to organic products, the EU accepts Israel's certification of such products for the purpose of exports to the EU as equivalent to EU standards. However, it does not recognise Israel's authority to carry out certifications beyond the pre-1967 lines. Following an EU request, Israel stopped certifying organic products that are grown, packed or processed in the occupied territories for the purpose of exports to the EU. Similarly, Israel is among third countries that are allowed to export certain products of animal origin (dairy and meat) to the EU on the basis of certification of animal and public health and veterinary conditions. Following the EU's request, Israel stopped exporting such products from the settlements to the EU.[14]
- **Consumer labelling**: In 2015, the European Commission issued guidelines on the origin indication of Israeli settlement products. Such products must not be labelled as "Made in Israel". Instead, they should be labelled as "Product of West Bank (Israeli settlements)" or "Product of Golan Heights (Israeli settlements)".[15]
- **Other areas**: In addition to the above, the EU has inserted territorial clauses excluding the occupied territories into other acts relating to areas of cooperation with Israel: marketing standards for fresh fruit and vegetables, Conformity Assessment and Acceptance of Industrial Products, imports of active substances for medicinal products, aviation, and

---

12 European Commission, EU-Israel Technical Arrangement, available at: https://ec.europa.eu/taxation_customs/business/calculation-customs-duties/rules-origin/general-aspects-preferential-origin/euisrael-technical-arrangement_en

13 European Commission, Guidelines on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards, 19 July 2013, available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/guidelines_on_the_eligibility_of_israeli_entities_and_their_activities_in_the_territories_occupied_by_israel_since_june_1967.pdf

14 EU Delegation to Israel, EU-Israel Trade Briefing, September 2016, available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/d-il/dv/201609eu-israeltradebriefing_/201609eu-israeltradebriefing_en.pdf

15 European Commission, Interpretative Notice (footnote 7 above).

exchange of personal data between Europol and Israeli authorities.[16] Among these is also the EU adequacy decision on personal data protection in Israel, which is discussed further below.

Importantly, the EU's differentiation policy has been validated by judgments of the **Court of Justice of the EU**. In its judgment on the *Brita* case in 2010, the CJEU confirmed the EU's right to exclude Israeli settlement products from preferential treatment under the EU-Israel Association Agreement.[17] In its judgment on the *Psagot* case in 2019, the CJEU reaffirmed the obligation to differentiate the consumer labelling of products from Israel, settlements and Palestinian products, thus validating the 2015 EU guidelines.[18] The CJEU has also upheld the differentiation principle in relation to another territorial conflict through its 2016 and 2018 judgments on *Western Sahara*, in which it ruled that EU agreements with Morocco are not applicable to Western Sahara.[19]

The EU's position, in accordance with international law and CJEU case-law, is unambiguous: it does not recognise the occupied territories as part of Israel and it considers Israeli settlements in those territories illegal. Accordingly, it has a policy of differentiation that seeks to ensure that any benefits accorded to Israel by the EU (e.g., in terms of trade) are not extended to the OTs.

The present paper addresses the question of how this policy 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 designation of Israel as a third country providing "adequate" protection to personal data in terms of EU data protection law.

- o – O – o -

[16] For a fuller overview, see European Council on Foreign Relations's Differentiation Tracker, available at: https://www.ecfr.eu/specials/differentiation-tracker

[17] CJEU, Judgment in Case C-386/08, *Firma Brita GmbH v Hauptzollamt Hamburg-Hafen*, 25 February 2010, available at: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-386/08

[18] CJEU, Judgment in Case C-363/18, Organisation juive européenne, Vignoble Psagot Ltd v. Ministre de l'Économie et des Finances, 12 November 2019, available at: http://curia.europa.eu/juris/document/document.jsf?docid=220534&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=15565554

[19] CJEU, Judgements in Case C-104/16 P, *Council v. Front Polisario*, 21 February 2016, and Case C-266/16, *Western Sahara Campaign*, 27 February 2018.

# 3. EU data protection law[20]

## 3.1 General

In Europe, the protection of fundamental rights of individuals in relation to the processing of their personal data – briefly, if somewhat misleadingly, referred to as "**data protection**" – is regarded as a fundamental human right. European data protection law requires all processing of personal data – from collection through use, disclosure and destruction – to be regulated by law, comply with a series of fundamental principles and "data quality" requirements, and be subject to independent oversight.[21]

At EU level, data protection is enshrined as a *sui generis* right in the EU Treaties (in particular Article 16 of the Treaty on the Functioning of the European Union, TFEU) and the EU Charter of Fundamental Rights (CFR) (Article 8). Detailed data protection rules were first issued for the EU "First Pillar" (the economic area) in 1995 in the form of a directive.[22]

In 2016, the EU adopted the General Data Protection Regulation (GDPR).[23] It came into application two years later, on 25 May 2018, replacing the 1995 Directive. The GDPR strengthened the already strong rules in the 1995 Directive on issues such as consent, the processing of sensitive data, data subject rights, profiling, data protection officers, etc..[24] It strongly reaffirmed the principle of accountability and introduced extensive record-keeping requirements through which controllers and processors of personal data must demonstrate their compliance.[25] It significantly strengthened the authorities charged with enforcing the rules, the so-called

---

[20] EU data protection law also applies to the three non-EU Member States of the European Economic Area (EEA), Iceland, Liechtenstein and Norway, hence the occasional references in the text to "EU/EEA" and "non-EU/EEA" countries – but I mainly simply refer to the EU. The brief overview of EU data protection law in this section is focused on the issues of transfers of personal data from the EU/EEA to non-EU/EEA countries ("third countries"). It does not address the issue of the direct applicability of the GDPR to controllers or processors in third countries (including Israel) that offer goods or services to individuals in the EU/EEA or that "monitor the behaviour" of such individuals (Article 3(2) GDPR), although there may well be entities in Israel to which the GDPR applies by virtue of that provision.

[21] See: Douwe Korff and Marie Georges, The Origins and Meaning of Data Protection, 13 January 2020, section 1.1, available at: https://ssrn.com/abstract=3518386

[22] Full title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995, pp. 31 – 50, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN
For details, see Douwe Korff and Marie Georges, The DPO handbook, Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, July 2019, Part One, section 1.3.2, available at:
http://www.fondazionebasso.it/2015/wp-content/uploads/2019/07/T4DATA-MANUAL-2019.pdf

[23] 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

[24] For a general introduction and overview (and a link to the recent Commission review of the GDPR after two years), see: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

[25] See Douwe Korff and Marie Georges, The DPO Handbook, (footnote 22, above), Part Two, section2.4.

supervisory authorities (previously more usually referred to as data protection authorities) and the body through which those authorities cooperate and issue EU-wide guidance, the European Data Protection Board (EDPB), the successor to the "Article 29 Working Party" (WP29) that was established under the 1995 Directive. And it introduced new mechanisms for cooperation and consistency in the supervisory authorities' actions. It also strongly reinforced the rules on transfers of personal data from the EU to "third countries", as discussed next.

## 3.2 EU Adequacy decisions and requirements for onward transfers[26]

### 3.2.1 The basic principle

Article 44 GDPR sets out the "general principle for transfers" of personal data to non-EU countries (so-called "third countries"), as follows:

*Article 44*

**General principle for transfers**

> Any transfer of personal data which are undergoing processing[27] or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined. (emphasis added)

Article 45(1) stipulates that:

> A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

---

[26] For further details, see section 2 of Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general, Part One of a submission to the EU bodies involved in assessing whether the UK should be granted a positive adequacy decision after the post-Brexit transition period, 9 October 2020, available at: https://www.ianbrown.tech/2020/10/09/the-uks-inadequate-data-protection-framework/
Section 2.2 of that submission describes the **process** for the adoption of an adequacy decision by the Commission.

[27] Note that "processing" here (and elsewhere in the GDPR) has a very broad scope, it covers: "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4(2) GDPR)

### 3.2.2 Requirements for a positive adequacy decision

The GDPR has introduced more specific and more demanding requirements in relation to transfers of personal data to non-EU/EEA countries than were in force when the Adequacy Decision on Israel was adopted in 2011, under the then in force 1995 Data Protection Directive. Moreover, the Court of Justice of the European Union (CJEU) has applied the relevant requirements strictly, as is reflected in new guidance on the matter from the European data protection authorities, noted below. Crucially, the Court of Justice of the European Union (CJEU) has held "adequate protection" must be read as requiring "essentially equivalent" protection to that accorded by EU law.[28]

#### i. Main matters to be taken into account

Article 45(2) sets out the main matters that the Commission must take into account in its assessment of the adequacy of the law in a third country.

Following the *Schrems I* "essential equivalence" test, the WP29 expanded on the requirements for an adequacy decision in its "Adequacy Referential", the final version of which was adopted in November 2017 and endorsed by the European Data Protection Board at its first meeting in May 2018.[29] Briefly, in line with the stipulations in Article 45(2), adequacy assessments must comprise the following three elements:

- an assessment of whether the law relating to privacy/the processing of personal data in the third country provides "essentially equivalent" protection to such data as is provided in the EU, in that they reflect the substantive "core content" elements of EU data protection law as summarised in Article 8(1) and (2) of the Charter of Fundamental Rights and further elaborated in the GDPR;
- an assessment of whether the law in the third country provides for "procedural/enforcement" guarantees that are "essentially equivalent" to those provided for Article 8(3) of the Charter and also further elaborated in the GDPR;

and, more broadly:

- an assessment of whether the rule of law and respect for human rights and fundamental freedoms is ensured in the third country concerned.

---

[28] CJEU, Grand Chamber judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems I*"), para. 73, available at: http://curia.europa.eu/juris/liste.jsf?num=C-362/14

[29] Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018 (WP254rev01), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
EDPB endorsement: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf
The 2017/2018 referential replaced very old previous guidance in the WP29 Working Document – Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive (WP12), adopted on 24 July 1998, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

## ii. Access to EU data by a third country's intelligence agencies

Article 45(2)(a) GDPR adds that the last of the above assessment elements, the one related to the rule of law, includes the question of whether the laws and rules in the third country relating to "*public security, defence, national security and criminal law and the access of public authorities to personal data*" are in line with the rule of law and respect human rights and fundamental freedoms as enshrined in EU law.

In 2016 (i.e. after *Schrems I*, but more importantly also after the Snowden revelations), the Article 29 Working Party issued a working document "*on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*,"[30] in which it set out important initial standards in that regard.

In July 2020, the CJEU issued its *Schrems II* judgment,[31] in which it assessed the surveillance regime of the USA with reference to EU fundamental rights standards, and found it wanting. In particular, access by the US national security agencies to personal data that are transferred to the USA is not limited to what is necessary and proportionate in relation to national security: US law allows for indiscriminate access to such data by those agencies, and provides no effective independent remedies to EU individuals who may be affected by those excessive US agencies' powers.[32] In two even more recent judgments, *Privacy International (PI)*[33] and *La Quadrature du Net (LQDN)*,[34] the Court provided further clarification on the fundamental EU legal requirements relating to mass surveillance.

Following these judgments, the European Data Protection Board, in November 2020, produced a recommendation containing a set of **updated** "**European Essential Guarantees for surveillance measures**" (hereafter: **EEGs**).[35]

---

30 WP29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted on 13 April 2016, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640363

31 CJEU Grand Chamber judgment in case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), 16 July 2020, available at: http://curia.europa.eu/juris/liste.jsf?num=C-311/18

32 See the Court's conclusions in paras. 184 – 185 and 197 of the judgment.

33 CJEU Grand Chamber judgment in Case C-623/17, *Privacy International*, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9CC0631635C4B49686319F07615E3E75?text=&docid=232083&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=10014575

34 CJEU Grand Chamber judgment in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10014575

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

## iii. Onward transfers

One related important matter is the question of "**onward transfers**", i.e., the onward transfer of personal data that have been exported from the EU to a country that has been held to provide adequate/essentially equivalent protection, to yet another third country that has not been so declared (and, where the adequacy decision is limited to a particular sector or category of recipients in the first "third country", also to any recipient in that first third country who is not covered by that decision). As we have seen, Article 44 GDPR now stipulates expressly that transfers, "*including onward transfers*", may only take place if it is ensured that the conditions set out in the GDPR are complied with, and more generally, that "*the level of protection of natural persons guaranteed by this Regulation is not undermined*."

This means that third countries cannot be held to provide adequate/essentially equivalent protection to personal data as is provided by the GDPR in the EU, unless their domestic law ensures not only such protection domestically, but also ensures that that protection continues if personal data that are imported from the EU are further, "onwardly" transferred to another country or recipient that is not covered by the adequacy decision.

Although this was already formally the position in 2011,[36] the matter has only recently been taken seriously. In most older adequacy decisions, it was barely addressed: the words "onward transfer" do not appear at all in the adequacy decisions on Switzerland (2000), Canada (2001),[37] Argentina (2003), Guernsey (2003), Isle of Man (2004), Jersey (2008), Andorra (2010), the Faroe Islands (2010), New Zealand (2012) and Uruguay (2012).[38]

In the 2011 adequacy decision on Israel, there is a stipulation in recital (14) that:

> Further onward transfers to a recipient outside the State of Israel, as defined in accordance with international law, should be considered as transfers of personal data to a third country –

---

The recommendations build on the earlier EEGs (WP237, footnote 30, above), but takes into account the important subsequent case-law of both the Luxembourg and Strasbourg Courts, in particular *Schrems II*.

**Note:** From now on, in this opinion, I will use the phrase "**undue access**" (by third country agencies, to personal data transferred to the third country from the EU) as shorthand for access by such agencies under laws or practices of the third country or territory concerned that do not meet the standards set out in these EEGs.

[36] The 1998 WP29 working document on transfers of personal data to third countries (WP12, footnote 29, above) already stipulated under the heading "**Restrictions on onward transfers**" that:
*"[F]further transfers of the [exported] personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive [i.e., with the provision on transfers based on 'appropriate safeguards' such as SCCs, now Article 46 GDPR]*".

[37] The WP29 Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, adopted on 26th January 2001 (WP39), does raise issues in this regard: see the section on *Interaction with Provincial legislation and Onward transfers* on pp. 5 – 6, but this is not reflected in the Commission Decision.

[38] Links to all these adequacy decisions can be found here:
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

but the implications are not spelled out (even though they are now significant, as I shall discuss in part 6, in the light of my findings in relation to the territorial application of the PPA, set out in part 5).

On the other hand, the two adequacy decisions on the USA (both now invalidated) did set out clear restrictions on onward transfers.[39] The EU-US Privacy Shield Decision may have been invalidated – but the above principle still stands and is indeed reinforced under the GDPR. This is made clear in the latest adequacy decision, on Japan,[40] issued in 2019 (the first to be issued under the GDPR). This has a whole section on onward transfers, section 2.3.9, that stipulates in its first paragraph (para. 75 in the decision) that:

> The level of protection afforded to personal data transferred from the European Union to business operators in Japan must not be undermined by the further transfer of such data to recipients in a third country outside Japan. Such "onward transfers", which from the perspective of the Japanese business operator constitute international transfers from Japan, should be permitted only where the further recipient outside Japan is itself subject to rules ensuring **a similar level of protection as guaranteed within the Japanese legal order**.
>
> (emphasis added)

In other words, **it is now explicitly clear that all adequacy decisions are inherently limited in their territorial scope to the third country or territory in question** (which in relation to all the other countries and territories that have been granted an adequacy decision raises no special issues, since unlike Israel none of them exercise their state powers outside of their internationally-recognised borders, let alone extend their data protection laws to territories outside of their internationally-recognised borders); and that all transfers from a third country or territory that has been held to provide adequate/essentially equivalent protection to another third country that has not been held to provide such protection constitute "onward transfers" for which special safeguards must be adopted.

In their relatively recent Adequacy Referential, the European data protection authorities stress two issues in this respect. First of all, that ensuring compliance with the onward transfer requirements lies squarely with the parties to the transfer, in particular the initial recipient in the

---

[39] Cf. the latest (2016) one: Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:TOC
The "special rules [that] apply to so-called 'onward transfers'" are set out in recitals (27) – (29) of that decision.

[40] 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, 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

country to which the data were originally transferred from the EU; and secondly, that onward transfers should be limited in scope.[41]

It should be stressed that the question of whether the other third country or the recipient in the first third country is subject to "rules ensuring a similar/adequate/essentially equivalent level of protection" to the EU is a matter for the EU to determine. The European Commission and the EU Member States' supervisory authorities are required to keep this issue under continuous review, and must intervene if they feel personal data sent from the EU to a country that has been held to provide adequate protection are at risk of losing the EU level of protection by disclosures to the first third country's agencies, or by onward transfers to other third countries

In section 4.1.5, at ii, below, I will note that the 2011 Adequacy Decision on Israel did not address the issue of onward transfers seriously; and in section 5.1.2, I will show that in fact the PPA, and practice under the PPA, in relation to onward transfers of personal data to the OTs seriously fails to comply with the requirements under the GDPR on onward transfers.

I will discuss the implications of the above findings in section 4.4.2, below.

### 3.2.3 Regular transfers in the absence of an adequacy decision[42]

According to Article 46 GDPR, routine or regular transfers of personal data to third countries that have not been held to provide adequate/essentially equivalent protection to such data may only take place provided that "appropriate safeguards" have been put in place. These can be put in place in particular in the form of contractual clauses between the EU-based data exporter and the third country-based data importer (Article 46 GDPR). The European Commission issued several sets of "Standard Contract Clauses" (SCCs) that could be used to that effect under the 1995 Data Protection Directive.[43] However, these SCCs were outdated, did not cover all situations, and did not reflect the higher standards set by the GDPR or the important case-law of the CJEU issued since they were adopted – especially the *Schrems II* judgment in which the CJEU made clear that such parties cannot simply rely on SCCs. Rather, data controllers and Member States' supervisory authorities must assess whether any transfer controllers make under such clauses may expose the data to undue access by the importing entities' state agencies, and/or whether there are inadequate remedies against such undue access in the relevant domestic law; and if

---

41 WP29, Adequacy Referential (footnote 28, above), section A.9, on p. 6.

42 Article 49 GDPR provides for derogations from the normal rules on transfers for special, non-regular, ad hoc transfers. The EDPB has issued guidelines on the (restrictive) applications of these derogations: EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf
However, since this opinion is concerned mainly with the general issue of data transfers from the EU/EEA to Israel and the OTs, we will leave these special derogations for occasional transfers aside. Suffice it to note that they cannot be relied on for transfers of personal data to Israeli authorities in response to decisions from Israeli authorities, courts or tribunals, because such transfers are prohibited by Article 48 GDPR (unless they are based on Mutual Legal Assistance Treaties, MLATs, or similar international agreements): EDPB Guidelines, p. 5.

43 See:
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

there are risks in these regards, they are required to adopt "supplementary measures" to effectively protect the data against such undue access.[44]

On 12 November 2020, in the light of this judgment, the European Commission issued **a new set of (draft) standard contract clauses** (or rather, a combination of general clauses and a selection of clauses in modular form that can be used to create more tailor-made contract schedules), to replace the SCCs issued under the predecessor to the GDPR, the 1995 Data Protection Directive.[45] In simple terms, they make clear that the data importer in the third country must **inform** the data exporter in the EU of any laws in the third country that do not "respect the essence of the fundamental rights and freedoms" guaranteed by the EU Charter of Fundamental Rights, and that "exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of [the GDPR][46] – as further clarified in the EDPB's updated "European Essential Guarantees for surveillance";[47] they must then consider whether the issue can be addressed by "supplementary measures" (and what those might be); and adopt appropriate, effective measures. If there are doubts as to whether the data can be effectively protected against undue access, the data exporter must **consult** the relevant EU supervisory authority; if the data cannot be effectively protected against undue access, **the export may not take place**.

Since the publication of the draft new SCCs, the EDPB has issued the **further guidance** anticipated in them.[48] This both provides for a **methodology** and expands on **what kinds of supplementary measures may be needed**. The EDPB gives as **examples**, the adoption of strong encryption (strong enough to ensure that the intelligence agencies of the third country cannot break it), or transferring only anonymised or strongly pseudonymised data (with, in both cases, only the EU exporter being able to de-encrypt or re-identify the data).

---

44 See the *Schrems II* judgment (footnote 31, above), paras. 133 – 135.

45 See:
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
The Commission has requested feedback on the clauses by 10 December and will no doubt revise them in the light of comments.

46 Article 23(1) covers in particular processing for the purposes of national security, defence, public security, law enforcement, and prevention of threats to public security.

47 Under the previous SCCs, any data importer in any non-adequate third country was already formally required to "warrant and undertake" that "*It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.*" However, in practice this was not enforced. This contrasts strongly with the new approach.

48 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, available at:
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Both aspects have obviously very significant implications in relation to transfers of personal data from the EU to Israel proper or the OTs (in the latter case, whether directly or indirectly, via Israel proper), as I will discuss in part 6, below.

- o – O – o -

# 4. The inadequacy of Israeli privacy law[49]

## 4.1 Inadequacy of the 2011 Adequacy Decision under the 1995 Data Protection Directive

### 4.1.1 Introduction

In 2011, the European Commission declared that the 1981 Israeli Privacy Protection Act 5741-1981, as amended in 2007 ("PPA"),[50] provided "adequate" protection in terms of the then applicable EU data protection instrument, the 1995 EC Data Protection Directive.[51] The decision was short (just six pages) and very basic, but based on a more extensive favourable opinion of the Article 29 Working Party, reached after quite extensive exchanges between the "Safe Harbour" sub-group of the WP29 and Israeli officials.[52]

The December 2009 WP29 opinion was based on the criteria for an adequacy assessment set out in a very early, 1998, WP29 Working Document,[53] that was replaced in 2017 by the much more demanding "Adequacy Referential", already mentioned.[54] Under the early – and now outdated – criteria, the WP29, and the EU Commission, were prepared to hold that a third country offered "adequate" protection if the rules in that country were roughly similar to those in the then-

---

[49] This part focusses on the Privacy Protection Act (PPA) and on the lack of safeguards against indiscriminate surveillance. Apart from the PPA, there are also the Protection of Privacy Regulations (Data Security) 5777-2017, unofficial English translation available at:
https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf
However, as the name indicates these really only deal with data security requirements and arrangements. The only issue in the Security Regulations that is mentioned in this part of my opinion is the classification of email addresses: see section 4.2.1, below. A set of other regulations issued under the PPA, relating to transborder data flows, is discussed in section 4.2, below.

[50] Protection of Privacy Law, 5741 – 1981, unofficial English translation available at:
https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf

[51] 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

[52] Article 29 Working Party, Opinion 6/2009 on the level of protection of personal data in Israel (WP165), adopted on 1 December 2009, available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf
The WP29 relied in part on a report commissioned by the EU Commission of the Centre de Recherches Informatique et Droit (CRID) of Namur University. The exchanges between the WPO and Israeli representatives took up most of 2009: see the background section in the opinion. It is not clear why the task was assigned to the "Safe Harbour" sub-group of the WP29, since that sub-group must have had as its mandate the EU – US "Safe Harbour" arrangement. Cf. also the report, A guide to data protection in Israel, produced in the context of an EU – Israeli Twinning Project, IS/2007/ENPAP/JH/01: *Strengthening Data Protection in Israel*, by Ian Bourne, Head of Data Protection Projects at the UK Information Commissioner's Office, in January 2010, available at:
https://www.gov.il/BlobFolder/legalinfo/legislation/en/AguidetodataprotectioninIsrael1.pdf

[53] WP12 (footnote 29, above).

[54] WP254rev01 (footnote 29, above).

applicable EU data protection instrument, the 1995 EC Data Protection Directive – or even, if they believed that the third country was in the process of moving closer to the EU rules.

In sections 4.1.2 and 4.1.3, below, I will briefly note this in relation to the first two main elements that must be addressed in any adequacy decision, i.e., the level of **substantive protection** accorded to personal data and the **"procedural/enforcement" guarantees** provided for.

In section 4.1.4, I will note that wider issues of **respect for the rule of law and human rights** were barely addressed, and not at all in relation to **access by Israeli agencies to transferred data from the EU**. In section 4.1.5, I will discuss how the issues of **territorial scope** and **"onward transfers"** – the focus of this opinion – were addressed in the 2011 decision. And in section 4.1.6, I will note that in spite of stipulations in the 2011 Commission Decision, the situation was not kept under review.

In section 4.2, I will then note the different assessments that are now required, under the GDPR and the recent "Adequacy Referential".

### 4.1.2 Substantive protection

There were a number of issue on which it was clear that even in 2011, Israeli law did not meet the substantive, "core", requirements of the then-applicable 1995 Data Protection Directive – but where the WP29 and the Commission accepted lower standards.

Thus, for example, the WP29 held in its 2009 opinion that "the definition of 'information' referred to in section 7 of the PPA is not similar to the definition set out in the Directive."[55] However:[56]

> Nonetheless, the Working Party takes into account the explanations given on this issue by the Israeli authorities and, in particular, the judicial precedents provided by them which imply an extension of the legal concept of information, making it similar to the concept of "data of a personal nature" within the meaning of the Directive.

In the same vein, the WP29 noted that the PPA only protects personal data in "databases" rather than all personal data that are processed by automatic means or which "form part of a [structured, manual] filing system or are intended to form part of [such] a filing system".[57] Consequently, it was "not possible to consider the Israeli legislation as adequate with regard to nonautomated or manual processing systems."[58] However, because reform in this respect had been proposed in the so-called "Schoffman Report", and because the area that was not adequate – manual processing of personal data – "will be residual", it felt that an adequacy decision could still be granted, as long as it did not apply to:[59]

> international data transfers whereby the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means.

---

55 WP29 Opinion on Israel (footnote 52, above), p. 4.

56 *Idem*, p. 5.

57 cf. Article 3(1) of the 1995 Directive and the definition of "'personal data filing system' ('filing system')" in Article 2(c)).

58 WP29 Opinion on Israel (footnote 52, above), p. 6.

59 *Idem*.

This was reflected in Article 1 of the 2011 Commission adequacy decision which only applied (and applies) to:

> personal data transferred from the European Union in relation to automated international transfers of personal data from the European Union or, where they are not automated, they are subject to further automated processing in the State of Israel.

The WP29:

> Recommend[ed] the adoption of provisions that envisage the application of Israeli legislation to manual databases as part of the legislative developments to be carried out in the future, and in particular in those related to the implementation of the "Schoffman Report", with the aim of being able to expand its assessment, where applicable, to include these processing systems –

but it did not feel the issuing of an adequacy decision (with the above-mentioned *caveat* in Article 1) needed to await those changes proposed by Schoffman. In fact, they have still not been implemented.[60]

The WP29 did not address the fact that protection under the PPA was (and is) limited to personal data in *registrable databases* – and that many databases need not be registered.

In relation to the core "purpose limitation" principle, the Israeli courts "have interpreted [the PPA] rules in similar terms to those envisaged by the Directive."[61] Similarly:

> With regard to the principle of quality in the strict sense, the Working Party believes that, even though it is not listed as an independent principle, the obligation of keeping the exact data and, if appropriate, keeping them up to date, is recognized by Israeli law through the regulation on the right to rectification referred to in Section 14 of the [PPA].

That, however, ignores the fact that a right to rectification of incorrect data is not the same as an independent duty on the part of the entity holding the data to ensure its correctness, etc.. Moreover, the right to correction under the PPA was (and is) more limited than under the EU rules. The WP29 dealt similarly lightly with the principle of proportionality, "welcom[ing] with satisfaction the clarifications given by the Israeli authorities", which referred to a few cases in the courts that were argued to effectively have applied the principle of proportionality through "the principles of reasonableness … and good faith." However, those cases concerned processing in the public sector only. Yet again, the WP29 was content to accept the promise of change based on the Schoffman Report that was never implemented:[62]

> Nonetheless, the Working Party believes it would [be] more satisfactory if Israeli legislation explicitly included this principle [proportionality], with the aim of guaranteeing that the activities that lie within the private sector and are different from those for which there are already court rulings based on the principles of reasonability and good faith, will be able to

---

60 DLA Piper, Data Protection Laws of the World – Israel, last modified 4 January 2020, p. 3, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=IL (click on link "DOWNLOAD current countries")

61 WP29 Opinion on Israel (footnote 52, above), p. 7.

62 *Idem*, p. 8.

> deal in the future with problems of interpretation that could hinder the adequate protection of the rights of the individuals involved. In this connection, the Working Party recalls that the inclusion of this principle within the PPA is contained in the conclusions of the "Schoffman Report".
>
> In this way, without the aforementioned conclusion affecting the final assessment regarding the level of protection of the State of Israel, the Working Party believes that the future legislative developments and, in particular, those related to the implementation of the "Schoffman Report", should adopt the provisions that envisage the express application of the principle of proportionality in relation to the totality of personal data processing carried out by the public and private sectors.

The WP29 also accepted that "the legislation of the State of Israel complies sufficiently with [the transparency principle]", even though the law only provides for the informing of data subjects when data are collected directly from them.

On the processing of sensitive data, the WP29 held that:[63]

> although [the list of sensitive data in section 7 PPA] does not fully coincide with the one established under Article 8 of the Directive, it may be regarded as similar.

The WP merely "urged" the Israeli authorities to consider as sensitive, data related to ethnic origin or sexual preferences, which are not included in the PPA list but important under EU law.[64]

The WP29 "confirmed" that the PPA allows for processing of personal data on the basis of implied consent, where the EU rules required (and still require) consent to be explicit – but felt that this was sufficiently remedied by the fact that under the PPA consent (including implied consent) had (and has) to be "informed":[65]

> Therefore, even though there is no rule similar to the one envisaged in the Directive, the Working Party believes the Israeli legislation adequately meets this principle.

On the restrictions on the taking of fully-automated decisions on individuals, which are not fully reflected in the PPA, the WP:[66]

> satisfactorily receive[d] comments contained in the report issued by the CRID and the clarifications carried out by the Israeli authorities in the sense that the Israeli law, in any event, enables the data subject to object to the adoption of these types of decisions.

Yet again, the prospect of reform sufficed:[67]

> without prejudice to considering this principle as met at this point in time, the Working Party urges the Israeli authorities to explicitly contemplate this principle in similar terms to Article 15 of the Directive in all future regulatory measures to be adopted regarding this matter.

---

63 *Idem*, p. 12.
64 *Idem*.
65 *Idem*.
66 *Idem*, p. 13.
67 *Idem*.

### 4.1.3 "Procedural/enforcement" guarantees (independent supervision)

In relation to supervisory and enforcement systems (referred to as "application mechanisms" in the WP29 opinion on Israel), the 1998 criteria did not yet require that the relevant authority be independent (as is now required under the 2017 Adequacy Referential). All the WP29 looked at at the time was whether there were "procedural/enforcement systems" that ensured "a good level of compliance" (with the law), "support and help to individual data subjects" and "appropriate redress" against breaches of the law.[68] In that respect, the WP concluded that the fact that the Database Registrar (since 2007 part of the Israeli Law, Information and Technology Authority, ILITA) was (and is) appointed by the Israeli government did not matter in view of certain safeguards that ensured, in the WP's view, that the supervisory agencies had:[69]

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

### 4.1.4 Respect for the rule of law and human rights

The WP29 opinion briefly notes that "*the so called 'Basic laws' [of the State of Israel] have been given constitutional status by the Supreme Court of Israel*"; that "*certain basic principles and fundamental human rights, such as equality, freedom of speech or freedom of religion, also have constitutional status*"; and that "*[w]ithin this framework, the right to privacy is included under section 7 of the Basic Law: Human Dignity and Liberty*" (p. 3). It then moves on to assess the PPA in the way noted in the previous sections.

The question of access to personal data by Israeli agencies including its national security agencies – and more specifically, of possible access by those agencies to data transferred from the EU – was **not addressed at all**.

### 4.1.5 Territorial scope and "onward transfers"

#### i. Territoriality

In its opinion the level of protection of personal data in Israel, the WP29 nowhere explicitly addresses the question of the territorial scope of the then pending adequacy decision. The issues of "the scope of territorial application of the draft decision and the exclusion of the occupied territories" were raised in the September 2010 meeting of the "Article 31 Committee", made up of Member States government representatives, and the Commission agreed to "prepare a further revised version to take account of the[se] issues".[70] A majority of the participating members of the committee voted in favour of a "slightly amended" version of the draft decision presented at the next meeting, in October 2010, but since some members were not present, no qualified majority was achieved, leading to a "no opinion" outcome that, however, still allowed the

---

68 See WP12 (footnote 29, above), p. 7.

69 WP29 Opinion on Israel (footnote 52, above), p. 14.

70 See the Summary record of the 54th meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee), 2 September 2010, available at: , https://ec.europa.eu/transparency/regcomitology/index.cfm

Commission to adopt its decision.[71] The Commission Decision on the adequacy of Israeli data protection law, as adopted, says:

*Article 2*

> 1. This Decision concerns only the adequacy of protection provided in the State of Israel, as defined in accordance with international law, with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC [i.e., the rules on transborder data flows] …
>
> 2. This Decision shall be applied in accordance with international law. It is without prejudice to the status of the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem, under the terms of international law.

There is some ambiguity in this, in that the text does not state explicitly that "the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem" are outside of "the State of Israel, as defined in accordance with international law". However, the legal position of the EU that these territories are not part of Israel under international law was already clear and unambiguous at that point and backed by the 2010 CJEU *Brita* judgment that pre-dates the 2011 Adequacy Decision on Israel: see section 2.2, above. The reference in the Adequacy Decision on Israel to "the State of Israel defined in accordance with international law" in 2011 could not then have been read (and still cannot be read) otherwise than as excluding the occupied territories.

Moreover, in view of the explicit commitment to "differentiation" subsequently adopted by the EU in December 2012 and applied in all other relevant EU acts since then, and further CJEU case-law (see section 2.1, above), Article 2(1) must certainly now, and arguably also already in 2011, be read as limiting the territorial scope of the adequacy decision to Israel within its 1967 internationally recognised borders and excluding all the occupied territories (even if Israel itself addresses the issue differently, as discussed in chapter 4, section 4.1, below).

However, the adequacy decision does not provide (and is not accompanied by) any guidance on *how* the territorial clause should be applied and respected in a situation where the Israeli government defines the territorial scope of Israeli law including PPA differently.

**In the light of the EU's legal position on the limitation of Israeli sovereignty to Israel proper, its "differentiation policy" and CJEU case-law, the 2011 Adequacy Decision on Israel must be read as not applying to processing of personal data in the OTs, outside of Israel proper, even if the Israeli PPA does apply to such processing.**

**Consequently, for the purposes of EU data protection law generally and the GDPR in particular, any direct transfer of personal data from the EU/EEA to the OTs must be treated as a transfer to a territory in which adequate protection of those data is <u>not</u> ensured; and any indirect transfer of personal data from the EU/EEA to the OTs via Israel must be regarded as an "onward transfer" of such data to such a non-adequate territory.**

[71] Summary record of the 55th meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee), 25 October 2010, available from the link in the previous footnote.

## ii. Onward transfers

As noted earlier, the early WP29 Working Document on transfers of personal data to third countries (WP12) of 1998 lists the issue of onward transfers as one matter that is to be assessed in an adequacy assessment, as follows:[72]

> **restrictions on onward transfers** - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.

At that time, the WP29 was of the opinion that:[73]

> most transfers of personal data to countries that have ratified Convention 108 [the 1981 Council of Europe Data Protection Convention] could be presumed to be allowable under Article 25(1) of the directive provided that:
>
> - the country in question also has appropriate mechanisms to ensure compliance, help individuals and provide redress (such as an independent supervisory authority with appropriate powers); and
> - the country in question is the final destination of the transfer and not an intermediary country through which the data are transiting, except where onward transfer is back into the EU or to another destination offering adequate protection.

Those two matters – the need for an independent supervisory authority and restrictions on onward transfers – were subsequently addressed in the 2001 Additional Protocol to Convention 108 of the Council of Europe.[74]

In this respect, the WP29 looked at the Privacy Protection (Transfer of Databases Abroad) Regulations adopted by the Government of Israel on 17 June 2001.[75] The WP noted that:[76]

> The regulations prohibit the transfer of data to third countries, unless those countries provide a level of data protection which is not less than that laid down in Israeli law, and specifically refers to several basic principles, such as lawful and legal collection and processing of data, purpose limitation, data quality (accuracy and keeping data up to date), respect for the right of access (and subsequently, according to Israeli legislation, rectification), and data security.
>
> Regulation 2(8) specifies several cases that could be considered as a legal presumption of adequacy, including Member States, those countries that are a Party to Convention 108 of

---

[72] Article 29 Working Party, Working Document – Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive (WP12) (footnote 29, above), Principle 6, on p. 6.

[73] *Idem*, p. 9.

[74] The Council of Europe Convention and its Additional Protocol are discussed in Douwe Korff and Marie Georges, The DPO Handbook (footnote 22, above), section 1.2.3.

[75] Unofficial translation into English available at: https://www.gov.il/BlobFolder/legalinfo/legislation/en/PrivacyProtectionTransferofDataabroadRegulationsun.pdf

[76] WP29 Opinion on Israel (footnote 52, above), p. 11.

> the Council of Europe[77] or those for which "the Registrar of Databases announced that an agreement has been achieved with a privacy agency of the third country".
>
> Paragraphs (1) to (7) of Regulation 2 specify several exemptions to these general rules:
>
> - *"if the data subject consented.*
> - *if it is impossible to have the consent, and it is crucial to transfer the data to protect the person's health.*
> - *if the data is transferred to a [foreign] corporation held by the owner of the [local] database, and he has guaranteed the data protection.*[78]
> - *if the receiver of the data has undertaken the obligation to provide data protection as if it were kept in Israel.*
> - *if the data is available to the public under a statutory authorization.*
> - *if the transfer is crucial to protect public order of safety.*
> - *if the transfer of data is required by Israeli law."*
>
> Regulation 3 states the accountability principle, which provides that the transferring party should arrange for the receipt of a guarantee from the receiver of the data that sufficient measures are undertaken to secure the data, and that such data are not further transferred.

The WP29, surprisingly – or perhaps not so surprisingly given that they never explicitly looked at the issue of territoriality – "believed" without any further analysis:[79]

> that the rules that have been set out comply with the principle of restriction of further data transfers to third countries and that the guarantees provided by the Israeli legislation on this issue make it possible to guarantee adequate respect for the rights of citizens of the European Union whose data are being processed in Israel.

Still, yet again, the WP29 hoped the issue would be better addressed in future:[80]

> Nonetheless, the Working Party would like to recall the criteria for the interpretation of exemptions established by Article 26(1) of the Directive and contained in its "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (document WP114) and it urges the Israeli authorities to carry out any interpretation of the exemptions contained in rule 2, previously mentioned, in accordance with the criteria included in the said document and in the Directive itself.

The list of exemptions in the 2001 Transfer Regulations (i.e., of conditions under which personal data may be transferred from Israel to a country [or territory?] where the level of protection is less than in Israel) has since been amended – but not in such a way as to bring them into line with EU data protection law: see section 4.3.2, below.

---

77 But note that Israel itself never became a party to Convention No. 108 or its Additional Protocol.

78 The words in square brackets were inserted by the WP29 – apparently without realising that they actually distort the effect of the exemption: see the discussion in the text.

79 *Idem*.

80 *Idem*, p. 12. The Working Document mentioned (WP114) was adopted on 25 November 2005. It is available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf
As noted in section 2.2.4, above, it has since been replaced by stricter guidance under the GDPR.

### 4.1.6 The absence of reviews of the 2011 adequacy decision

As noted above, the WP29 established that in relation to several issues – such as the application of the PPA to manual databases, the lack of clarity about the application of the proportionality principle to processing in the private sector, and the interpretations of the exemptions relating to international data transfers online – the Act could not really be said to meet the same standards as the then-applicable 1995 Data Protection Directive. However, it still supported the issuing of a positive adequacy decision, merely "urging" the Israeli authorities to take steps to bring their law more in line with the EC Directive. It added that:[81]

> within the framework to be established by the Decision finally adopted by the Commission, it **[the WP] will closely follow the measures adopted** within the framework of the issues.

The 2011 Adequacy Decision on Israel did not preclude action if such entreaties were left unanswered. Rather, Article 3(1)(b) stipulates the following:[82]

> *Article 3*
>
> 1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to a recipient in the State of Israel in order to protect individuals with regard to the processing of their personal data in the following cases:
>
>    (a) …
>
>    (b) where there is a substantial likelihood that the standards of protection are being infringed, there are reasonable grounds for believing that the competent Israeli authority is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the party responsible for processing established in the State of Israel with notice and an opportunity to respond.
>
> 2. The suspension shall cease as soon as the standards of protection are assured and the competent authority of the Member States concerned is notified thereof.

The Commission, in its adequacy decision, also promised in Article 5 that:

> **The Commission shall monitor the functioning of this Decision** and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC,[83] including any evidence that could affect the finding in Article 1 of this Decision, that protection in the State of Israel is adequate within the meaning of Article 25 of Directive 95/46/EC and any

---

81 WP29 Opinion on Israel (footnote 52, above), p. 18 emphasis added.

82 This is a standard clause, also included *verbatim* in the adequacy decisions on Canada (2001, Article 3), Argentina (2003, Article 3) and Andorra (2010, Article 3), and in less explicit terms in the adequacy decisions on the USA (2016 – the now invalidated Privacy Shield decision, Article 3 and 4(3)) and Japan (2019, Article 2 and 3(3)).

83 The "Article 31 Committee" was composed of representatives of the EU Member States.

> evidence that this Decision is being implemented in a discriminatory way. In particular, it shall monitor the processing of personal data in manual databases. (emphasis added)

**But in fact, no further action was ever taken under these clauses by either the WP29 or its successor, the EDPB, or the Commission, since the adoption of the decision.**

Finally, it should be noted that the GDPR stipulates that:

> Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted [under Article 45 GDPR]. (Article 45(9)).

The 2011 decision has therefore been allowed to operate unchallenged for almost a decade, in spite of the above-mentioned deficiencies – and even since the coming into application of the GDPR, under which those deficiencies are even more glaring (as discussed next).

## 4.2 Inadequacy of the PPA under the GDPR

### 4.2.1 New standards, same old law (for now)[84]

On the EU side, since the 2011 adequacy decision, several important matters have occurred (as noted in section 2.2, above):

- The CJEU has ruled that an assessment of the adequacy of a third country's system of protection of personal data must entail an assessment, not of whether the rules and practices in the third country are "similar" to the EU rules, or moving in that direction, but a much more demanding assessment of whether those rules and related practice in the relevant third country ensure "essentially equivalent" protection to the EU rules; and
- The 1995 EC Data Protection Directive has been replaced by the stricter and much more demanding GDPR – which means that third countries' laws and practices must now be measured against the rules in and the practices under the Regulation, rather than its weaker predecessor.

At the same time, the Israeli Privacy Protection Act has changed little, if at all. The PPA itself has not been substantially amended since 2007 (i.e., since before the EU adequacy decision). In 2018, the Israeli Privacy Protection Regulations (Data Security), 5777-2017, entered into force at the same time the GDPR came into effect, in May 2018.[85] However, as already noted in section 4.1.1, above, these Regulations are effectively limited to strengthening the security requirements of the law only; they do not otherwise bring the PPA in line with the GDPR. Otherwise, according to critics:[86]

---

84 In section 4.2.3, below, we note some very recent proposals for amendments to the PPA that relate to the status and powers of the Israeli Privacy Protection Authority.

85 See footnote 49, above.

86 *On Anniversary of GDPR Enactment, Israel's Privacy Laws Still Far Behind*, Calcalistech, 25 May 2020, at: https://www.calcalistech.com/ctech/articles/0,7340,L-3826990,00.html

> Israel has struggled to keep its privacy policies updated, despite its global position as a small yet worthy tech hub and a leading developer of data processing technologies. The country's privacy laws are embarrassingly outdated, as Israel's Privacy Protection Act has had very few amendments since 1981.

In the light of these matters, and given the significant weaknesses in the original EU assessment of Israeli law (as outlined in the previous section), **it is manifest that the Israeli Privacy Protection Act fails to meet the GDPR standards in many serious respects.** Without pretending to provide a comprehensive analysis (which is beyond the scope of this paper and unnecessary in view of the many manifest deficiencies in the PPA), below are listed a number of the most glaring deficiencies (from an EU point of view) in relation to the first two matters that must be addressed in an adequacy assessment under the new "Adequacy Referential":[87] whether the PPA reflects the substantive "core content" elements of EU data protection law in an "essentially equivalent" manner (section 4.2.2, below); and whether the status and powers of the Privacy Protection Authority under the PPA ensures "essentially equivalent" "procedural/enforcement" protection (section 4.2.3, below). The third element, concerning broader adherence to the rule of law, more specifically in relation to access to transferred data by Israeli national security agencies, is discussed in section 4.2.4, below. The related issue of "onward transfers"[88] is discussed in part 5, in the broader context of the territorial application of the PPA.

Some of the deficiencies were already noted by the WP29 (but glossed over), while others only become apparent in relation to the new, higher standards in the GDPR and set by the CJEU.

### 4.2.2 Inadequacies in terms of the "core" substantive requirements

The following are the most glaring deficiencies in the PPA compared to the EU GDPR:

- Broader remit:

  Although the PPA also covers (most) processing of personal information (see below), it has a broader privacy remit, addressing also *inter alia* "spying on or trailing a person" in a harassing way, listening in to a person contrary to any law, photographing a person while in a private domain, copying or using the contents of someone's letters, using a person's name, picture or voice for profit, etc. (section 2). This results in less focus on protection of personal data – data protection – as a *sui generis* right (as it is regarded in the EU: see Article 8 of the EU Charter of Fundamental Rights).

- More limited material scope:

  As its very title, "Protection of Privacy in Database[s]", makes clear, all the specific data protection provisions in Chapter Two of the PPA are limited in material scope to registered databases and the use of personal information in registered databases. This is much more limited than the material scope of the GDPR, defined in Article 2(1) as follows:

---

87 See section 3.2.1 and footnote 29, above.

88 See section 3.2.3, above.

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
>
> (A "filing system" being defined as, essentially, any structured collection of personal data including structured manual/paper collections of data: see Article 4(6).)

In particular, whereas the only real exclusions from the scope of the GDPR are processing by a natural person in the course of a purely personal or household activity (which is restrictively interpreted) and processing in relation to national security,[89] the PPA does not cover any use of personal information that is not contained in a registrable database – and databases containing information on less than 10,000 persons do not need to be registered unless they contain sensitive data (as rather narrowly defined: see below), or include information on the data subjects that "was not delivered to this database by them, on their behalf or with their consent to this database", or are used for direct mailing (section 8(c)). That leaves very significant gaps in protection.

- More limited in terms of acts deemed an infringement:

The PPA defines as an infringement of privacy, in addition to the ones listed in the first indent, above:

> using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given; and
>
> publishing any matter relating to a person's intimate life, including his sexual history, state of health or conduct in the private domain.
>
> (Section 2(9) and (11))

It would appear as a matter of simple linguistics that neither the term "use" nor the term "publishing" covers **collecting** or **storing** (including mandatory **retention**) of personal data. Those actions are therefore not included in the acts that are in principle prohibited under the PPA (subject to exceptions). This is actually a major issue in the EU, in particular in relation to mandatory data retention and untargeted surveillance based on collection of communications data in bulk.[90] Cf. the broader definition of "processing" (of personal data) in the GDPR that covers "any operation or set of operations which is performed on

---

[89] Most other matters excluded from the GDPR – processing in relation to law enforcement and processing by the EU institutions – are subject to separate instruments that in essence follow the GDPR. Processing of personal data in relation to the EU's external affairs still needs to be brought into line with the GDPR. Processing of personal data for national security purposes by EU Member States is outside EU competence – but the making available of data that are subject to the GDPR to national security agencies is subject to the GDPR. And the CJEU stressed in no uncertain terms in *Schrems II* that the national security exemption in the EU Treaties does not apply to processing of personal data for such purposes by non-EU/EEA (third) countries. See para. 81 of the judgment.

[90] See EDRi's Data Retention: Revisited booklet, published on 28 September 2020, for an overview of the issues, available at:
https://edri.org/our-work/launch-of-data-retention-revisited-booklet/

personal data or on sets of personal data" including collection, storage, use, disclosure and destruction.[91]

In its *Digital Rights Ireland* judgment, the Court of Justice of the EU stressed that mandatory data retention was in itself an interference with the right to data protection (and this applies by extension also to collection), with access to – and use of – the retained (or collected) data constituting a "further interference".[92] Consequently, each of the above-listed acts – collection, storage, accessing and use of personal data – are subject to the constraints of the GDPR, such as the need for an appropriate legal basis, purpose-specification and -limitation, necessity and proportionality, data minimisation, etc.

- Less strict in relation to consent:

The PPA defines "consent" as follows:

> "consent" means informed, express or implied consent.
>
> (Section 3)

This contrasts sharply with the GDPR definition of consent:

> "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
>
> (Article 4(11))

This is further extensively expanded upon in Article 7 ("Conditions for consent"). Under the GDPR, consent cannot be deduced from inaction ("*By continuing on this website, you consent to the use of your data in accordance with our privacy policy*"). For the processing of so-called "special categories of data" ("sensitive data"), "explicit" consent is in any case required. Moreover:

- More limited categories of sensitive data:

The GDPR lays down stricter rules on the processing of certain special categories of personal data (usually referred to as "sensitive data" than on the processing of other, non-sensitive data. The categories of data subject to the stricter rules are, first of all:

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data (when processed for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation
>
> (Article 9(1) GDPR)

---

91 See footnote 27, above.

92 See CJEU Grand Chamber judgment in Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland*) of 8 April 2014, paras. 34 – 35, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

Also subject to special restrictions is processing of "personal data relating to criminal convictions and offences or related security measures" (Article 10). Processing of national identification numbers or "any other identifier of general application" must also be specifically regulated (Article 87).

The PPA contains two references to data that are subject to special constraints, but those categories are clearly much more limited than the EU ones. Section 2(11) of the PPA refers to:

> matter[s] relating to a person's intimate life, including his sexual history, state of health or conduct in the private domain

And section 7 PPA defines "sensitive information" as:

> data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person.

The definitions in the sections quoted above do not appear to include race or ethnic origin (as the WP29 also noted), or trade union membership (which it did not).

On the other hand, information on a person's "economic position" is not formally included in the list of sensitive data in the GDPR – but the European supervisory authorities still tend to stress the need for special care in processing such information.

Moreover, as noted earlier, the PPA only makes "publishing" of the intimate matters contrary to the law, rather than any processing of sensitive data under the GDPR (subject to exceptions).

- <u>Underpinned by a system of registration that has been abandoned in the EU because it was ineffective as a means of ensuring compliance</u>:

  The PPA is still based on a system of notification and registration of databases. That was also the basis for the 1995 EC Data Protection Directive – but it was abandoned in the GDPR because it had proven to be of little use, and replaced by a new (or at least much stronger) principle of accountability, with important duties placed on controllers (and to a lesser extent processors) in terms of record-keeping, mandatory risk assessments, in-depth data protection impact assessments and mandatory consultation with the supervisory authorities in some cases, etc..

  It is difficult to see how a registration-based system can be said to offer "essentially equivalent" protection to an accountability/record-keeping system when the EU has determined that the former does not work.

- <u>Less rights for data subjects</u>:

  The PPA sets out just three rights: the right of any person to "inspect" information on him/her in a registered database (section 13); the right to request changes to the information if the information is "not correct, not complete, not clear or not up to date" (section 14); and the right to appeal to a court if access or amendment is refused (section

15). But there are no such rights in relation to information that may be held in databases or data collections that need not be registered (see *Material scope*, above).

Moreover, the GDPR grants a much broader range of rights:

- Right to be informed of processing (Arts. 12 – 14);
- Right to a free copy of one's data (Art. 15);
- Right to rectification of inaccurate or incomplete data (Art. 16);
- Right to erasure ("right to be forgotten") (Art. 17);
- Right to restriction of processing (i.e., to have contested data blocked) (Art. 18);
- Right to have recipients of data informed of corrections (Art. 19);
- Right to data potability (Art. 20);
- Right to object to processing (Art. 21);
- Right not to be subject to fully-automated decisions/profiling (Art. 22).

- Excessive exemptions:

Even when the PPA applies (see above, *Material scope*), there are broad exemptions in the Law:

- "No person shall bear responsibility under this Law for an act which he is empowered to do by law" (section 19(a)); and
- The Israeli police and security agencies and anyone working for them "shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of carrying them out (section 19(b)).

This contrasts with the derogation clause in the GDPR, Article 23, which only allows for restrictions on the rights of data subjects by law and:

> when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard [national security, defence, public security, criminal law activities, etc.].

More specifically, Israeli law does not provide for appropriate limitations on mass surveillance: see section 4.2.4, below.

**IN SUM: The PPA is glaringly deficient in terms of the substantive "core" EU data protection standards and offers far from "essentially equivalent" protection in this regard compared to the GDPR.**

### 4.2.3 Inadequacies in terms of "procedural/enforcement" requirements

#### i. The current situation

The 2009 WP29 opinion on Israel, adopted under its 1998 working document on transfers, WP12,[93] noted that the Database Registrar, which was then the Israeli data protection authority, had been integrated in the Israeli Law, Information and Technology Authority (ILITA) that also housed the Certification Authorities Registrar and the Credit Data Services Registrar and that, as a result of certain modifications:[94]

> [The Head of ILITA], and therefore the said authority [the Database Registrar], [were granted] **an adequate degree of independence** for the purposes that are established for supervisory authorities regulated by the Directive. In particular, it takes into account that those who integrate ILITA and its Head have the profile of civil servants, and are not subject to any type of mandate or political profile.

The WP29 also found that "[budgetary] assignations given in the last few years make it possible to consider its status of independence as adequate".[95] Moreover:[96]

> the competencies attributed to ILITA", which even include the prosecution of criminal offences against privacy, and the fact that ILITA has been designated to organize the 32nd International Conference on Privacy and Personal Data Protection, which is scheduled to be held in Jerusalem in October 2010, reinforce the efforts made by the State of Israel to guarantee the existence of a personal data protection authority and to adequately safeguard this right.

However, the independence and powers of the current authority, the Privacy Protection Authority, cannot be as generously assessed under the new "Adequacy Referential". In particular, the fact that the Privacy Protection Authority is still under the authority of the Ministry of Justice and does not report directly to Parliament, raises serious doubts about its independence

This is clear from the 2012 CJEU judgment in *European Commission v. Austria*,[97] in which the Court held that the Austrian data protection commission (*Datenschutzkommission*, DSK) was not independent in terms of the 1995 Data Protection Directive because the managing member of the DSK was a federal official subject to administrative supervision, the office of the DSK was integrated with the departments of the Federal Chancellery, and the Federal Chancellor had an unconditional right to information covering all aspects of the work of the DSK.[98]

---

93 See footnote 29, above.

94 WP29 Opinion 6/2009 (footnote 52, above), p. 14, emphasis added.

95 *Idem*, p. 15.

96 *Idem*.

97 CJEU Grand Chamber judgment in Case 614/10 (*European Commission v Republic of Austria*), 16 October 2012, available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62010CJ0614

98 Summary of conclusions in para. 68.

**IN SUM: The PPA is also deficient in terms of the "procedural/enforcement" EU standards, in particular in terms of the limited independence of the Privacy Protection Authority, which is not "essentially equivalent" to the level of protection and independence required of EU Member States' supervisory authorities under the GDPR.**

### ii. Proposed changes

On 19 August 2020, a series of draft laws were presented to the Israeli Parliament, the Knesset.[99] This includes a set of proposed amendments to the PPA.[100] These all relate to the tasks and powers of the Privacy Protection Authority, and to administrative supervision over the processing of personal data by security agencies. In relation to the former, it proposes training and certification of PP Authority investigators and supervisors; distinguishing between supervisory powers, powers of administrative inquiry and criminal investigation; giving the Authority the power to issue infringement notifications to entities violating the PPA and orders requiring them to cease violations, and powers to impose administrative fines and to commence prosecutions. It is also proposed to make certain violations of the PPA more serious criminal offences.

As concerns the security agencies, it proposes supervision by an "internal privacy inspector" rather than the PP Authority; the internal inspector is merely to "report his findings" to the Authority.

However, there is no certainty as to whether, and if so how, the proposed changes may be implemented.

Although it would appear that the Government intends to strengthen to Act in some respects in relation to supervision and enforcement, in the circumstances it is not yet possible to assess whether the changes are likely to meet the EU "procedural/enforcement" standards. The proposals for "internal" supervision over the collection and use of personal data by the security agencies in particular will require very careful examination of the final legal details (which are not yet available). For now, these proposals are merely suggestions of change, and in relation to the security agencies dubious change. They cannot be relied upon in relation to any decision on the adequacy of Israeli privacy law by the EU Commission.

## 4.2.4 Inadequate protection against indiscriminate surveillance

### i. Introduction

Quite separate from the general deficiencies in the PPA compared to the GDPR noted in the previous sections, there is the major issue of access by Israeli security agencies to data transferred from the EU/EEA to the State of Israel or the OTs in an economic context. As noted in section 3.2.2, above, in *Schrems II*, the Court of Justice of the EU has held that a non-EU (third) country

[99] See: https://www.gov.il/BlobFolder/reports/seder_hakika190820/he/seder_Hakika_sederHakika230820.pdf

[100] See pp. 1 – 41.

cannot be declared to provide "adequate" protection to personal data in terms of the GDPR if the law of that country allows the security agencies indiscriminate access to such data, and/or does not provide for appropriate, independent and effective remedies. In its *PI* and *LQDN* judgments, the Court further clarified the EU fundamental rights standards relating to mass surveillance and access by intelligence agencies to bulk communications data including the need for strict limitations on the use of broad surveillance powers and for close supervision and effective remedies.[101]

This is again not the place for a comprehensive assessment of Israeli surveillance law or practices against those standards. But such information as there is clearly shows that Israeli rules and practices relating to surveillance over e-communications are not constrained in ways that would make them compatible with the EU standards – either in Israel proper, East Jerusalem and the Golan Heights (to which Israeli domestic surveillance laws apply equally), or in the West Bank (where there is ubiquitous surveillance, subject to few legal constraints). Moreover, there is an issue in relation to surveillance relating to foreigners outside Israel or the OTs, including EU persons, who are seen as opponents of Israeli policies. The latter issue is relevant in particular in relation to monitoring of communications between such foreigners and individuals in Israel or the OTs.

Before turning to these specific contexts in sub-sections iii - v, I first, in the next sub-section, briefly describe the general capabilities and practices of the Israeli agencies involved in the surveillance, in particular the Israeli Defence Force (IDF) Unit 8200, on the basis of an analysis of publicly available information by the ETH Centre for Security Studies.[102]

### ii. Israeli surveillance capabilities and practices

The main IDF unit responsible for surveillance over electronic communications is Unit 8200, Israel's signals intelligence (SIGINT) unit, roughly equivalent to the United States' National Security Agency (NSA) and the UK's General Communications Headquarters (GCHQ).

According to the ETH report:[103]

---

101 For details, see Lorna Woods, *When is mass surveillance justified?*, EUlawanalysis blog, 7 October 2020, available at: https://eulawanalysis.blogspot.com/2020/10/when-is-mass-surveillance-justified.html
Also Graham Smith, *Hard questions about soft limits*, Cyberleagle blog, 15 October 2020, available at: https://www.cyberleagle.com/2020/10/hard-questions-about-soft-limits.html
I am focussing on surveillance over electronic communications including mobile communications and the Internet because that kind of surveillance is most relevant to transfers of personal data from the EU to Israel and the OTs. However, in section iii, below, I will also briefly note the extensive offline surveillance in the OPT, and the link between this offline- and online surveillance.

102 The Israeli Unit 8200: An OSINT-based study, ETH, Zurich, 2019, available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf

103 *Idem*, section 5.1, *Strengths*, on p. 16, emphases added.

> [Unit 8200] maintain[s] and operate[s] an **extensive infrastructure** (with advanced technologies from antennas to satellites) and large-scale bases (with the Urim base, for example, being **one of the world's largest SIGINT bases**)[104] …
>
> [I]n addition to technology, the Unit has, over the past decades, developed considerable intelligence and cyber capabilities. As such, it now possesses an institutional know-how and memory that very few nations can compete with …

More specifically:[105]

> [T]he Unit's SIGINT activities cover a wide range of tasks from the analysis of information in the public domain to the use of human operators and special signal intelligence.[106] Unsurprisingly, they also comprise the **interception of various types of communications** (i.e. spying), their translation, decryption and analysis. ...
>
> … *Le Monde Diplomatique* claimed in 2010[107] that the Unit was operating a massive international spying and listening network through its various SIGINT bases. Indeed, thanks to its large antennas and receptors, its Urim base ( … ) is apparently able to **monitor the phone calls, emails, and other communications of both friendly and enemy nations across the Middle East, Europe, Asia, and Africa**. According to the same article, the Urim base also has the infrastructure to **tap underseas cables** (e.g. Mediterranean cables linking Israel to Europe via Sicily) …

Moreover:[108]

> The Israeli intelligence community is widely known to cooperate with its partners, which often include Britain, Canada and the US.[109]
>
> According to various leaks, including the Snowden leaks, Unit 8200 has developed a close partnership with the latter and its NSA.[110] Indeed, according to leaked documents, the NSA "maintains **a far-reaching technical and analytic relationship** with the Israeli SIGINT National Unit (ISNU) [aka. Unit 8200] sharing information on access, intercept, targeting, language, analysis and reporting.".[111] Furthermore, and among others, both agencies signed

---

104 For details of this base, see pp. 11 – 12 of the ETH report.

105 *Idem*, p. 8, emphases added.

106 Reed, J., 2015, Unit 8200: Israel's cyber spy agency [WWW Document]. Financ. Times. URL: https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c [original note]

107 Hager, N., 2010, Israel's omniscient ears [WWW Document], Monde Dipl. URL: https://mondediplo.com/2010/09/04israelbase [original note]

108 The Israeli Unit 8200: An OSINT-based study (footnote 102, above), pp. 9 – 10, emphases added.

109 Sledge, M., 2014, NSA Has 'Far-Reaching' Partnership With Israeli Intelligence Agency [WWW Document], Huffington Post. URL: https://www.huffpost.com/entry/nsa-partnership-israel_n_5646263?guccounter=1 [original note]

110 Greenwald, G., 2014, *Cash, weapons and surveillance: the U.S. is a key party to every Israeli attack* [WWW Document], The Intercept. URL: https://theintercept.com/2014/08/04/cash-weapons-surveillance/ [original note]

Sledge, M., 2014 [see previous footnote; original note]

111 Greenwald, G., Poitras, L., MacAskill, E., 2013, *NSA shares raw intelligence including Americans' data with Israel* [WWW Document]. The Guardian. URL: https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents [original note]

> a memorandum of understanding in 2009, in which they agreed that the NSA would provide the Unit with raw American SIGINT.[112] This included but was not limited to, "unevaluated and unminimized transcripts, gists, facsimiles, telex, voice and **Digital Network Intelligence metadata and content**.".[113]
>
> …
>
> In addition to the above cooperations, Unit 8200 probably works with many more of its peers, however, there is currently no relevant information in the public domain.

The reference in the above-mentioned NSA document to a "far-reaching analytical relationship" between Unit 8200 and the US's NSA, and references by Arik Brabbing, a former head of the Shin Bet's Cyber Directorate, to "big data analyses",[114] clearly indicate that Unit 8200 is involved in bulk e-communications data collection and algorithmic/AI-based analyses of those data, similar to those carried out by the USA's National Security Agency (NSA) and the UK's Government Communications Headquarter (GCHQ), as exposed by Edward Snowden.[115]

The relevant advanced capabilities in this regard appear to be often developed by private Israeli companies with very close links to the agencies, and Unit 8200. For instance, the Israel-based technology firm NSO Group Technologies, whose founders are ex-members of Unit 8200, developed spyware called *Pegasus* that enabled the remote surveillance of smartphones.[116] In 2019, the company was sued by instant messaging company WhatsApp and its parent company Facebook under the US Computer Fraud and Abuse Act (CFAA).[117] The software could

---

112 Bamford, J., 2014, *Israel's N.S.A. Scandal* [WWW Document]. N. Y. Times. URL: https://www.nytimes.com/2014/09/17/opinion/israels-nsa-scandal.html

NSA, 2009, Memorandum of Understanding (MoU) between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli Sigint National Unit (ISNU) Pertaining to the Protection of U.S. Persons. [original note]

113 Greenwald et al., 2013 [footnote 111, above; original note]

114 See footnote 125, below, and the quote in section iii.

115 For a write-up of GCHQ's activities in this regard, see Open Rights Group, GCHQ and UK Mass Surveillance, Part One, Chapter One, *Passive collection*, and Chapter Three, *Putting mass surveillance to use*, available at: https://www.openrightsgroup.org/app/uploads/2020/03/01-Part_One_Chapter_One-Passive_Collection.pdf and: https://www.openrightsgroup.org/app/uploads/2020/03/03-Part_One_Chapter_Three-Analytics_and_usage.pdf
The UK activities are assessed under the EU fundamental rights standards in Douwe Korff and Ian Brown, The inadequacy of UK data protection law in general (Part One, footnote 26, above) and in view of UK surveillance (Part Two), available at:
https://www.ianbrown.tech/2020/11/30/the-uks-intelligence-activities-and-gdpr-inadequacy/
See also the Executive Summary of that submission that contains a discussion of the implications of the findings, available at:
https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf
The Korff/Brown analysis of UK surveillance practices with reference to the EU standards (in particular, the "European Essential Guarantees" for surveillance) is relevant to Israel because Israel appears to be carrying out very similar surveillance activities and, also like the UK, carries out those activities in close cooperation with the USA.

116 See: https://en.wikipedia.org/wiki/NSO_Group

117 The WhatsApp-NSO Group Lawsuit and the Limits of Lawful Hacking, Lawfare blog, 5 November 2019, available at:

surreptitiously gain access to a phone's camera, microphone, text messages, emails and location information. The *Pegasus* spyware is classified as a weapon by Israel and any export of the technology must be approved by the government.[118]

Given the close links between the Israeli security agencies and this company – and other Israeli companies that develop advanced surveillance software – it is inconceivable that the agencies are not using these capabilities, at least in the OPT, especially given the almost complete absence of regulation of such technologies in the territory, noted in the next sub-section.

**In sum:**

**The Israeli security agencies, in particular SIGINT Unit 8200, have highly advanced surveillance capabilities, often developed by Israeli companies that are at the forefront of such technologies globally, that enable them to access mobile communications and underseas cables that form part of the global Internet infrastructure; and to perform algorithm/AI-based datamining analyses of the bulk data so captured. In other words, they have similar capacities to those of the US's NSA and the UK's GCHQ, exposed by Edward Snowden – and the Israeli agencies in fact work closely with at least the US's NSA in this regard.**

### iii. Surveillance in the Occupied Palestinian Territory

It has been clear for some years that the Israeli authorities, in particular Unit 8200, have been carrying out mass surveillance over the Palestinian population in the OPT. Some years ago, reports and criticism were focused on offline mass surveillance, in particular after 43 Unit 8200 veterans in 2014 voiced their concerns in a public letter to the chief of staff of Israel's armed forces and also the head of military intelligence. To quote from the UK *Guardian* report on the letter:[119]

> The signatories say … that a large part of their work was unrelated to Israel's security or defence, but appeared designed to perpetuate the occupation by "infiltrating" and "controlling" all aspects of Palestinian life.
>
> Written in uncompromising language the letter states: "We, veterans of Unit 8200, reserve soldiers both past and present, declare that we refuse to take part in actions against Palestinians and refuse to continue serving as tools in deepening the military control over the Occupied Territories."

https://www.lawfareblog.com/whatsapp-nso-group-lawsuit-and-limits-lawful-hacking

[118] *Spyware technology found on phone of Moroccan journalist, report says*, Washington Post, 21 June 2020, available at: https://www.washingtonpost.com/investigations/spyware-technology-found-on-phone-of-moroccan-journalist-report-says/2020/06/21/ca409294-b220-11ea-8758-bfd1d045525a_story.html

[119] *Israeli intelligence veterans refuse to serve in Palestinian territories: Innocent people under military rule exposed to surveillance by Israel, say 43 ex-members of Unit 8200, including reservists*, *Guardian*, 12 September 2014, available at: https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories

They add: "The Palestinian population under military rule is completely exposed to espionage and surveillance by Israeli intelligence. It is used for political persecution and to create divisions within Palestinian society by recruiting collaborators and driving parts of Palestinian society against itself. In many cases, intelligence prevents defendants from receiving a fair trial in military courts, as the evidence against them is not revealed."

Accompanying the letter – published in the Israeli media on Friday, and organised several months before the recent Gaza war – are a series of testimonies provided by the signatories to Yedioth Ahronoth and shared with the Guardian.

A common complaint, made in both the testimonies and in interviews given by some of the signatories, including to the Guardian this week, is that some of the activities the soldiers were asked to engage in had more in common with the intelligence services of oppressive regimes than of a democracy.

Among allegations made in the statements are that:

- A significant proportion of the unit's Palestinian objectives "are innocent people unconnected to any military activity. They interest the unit for other reasons, usually without having the slightest idea that they're intelligence targets." According to the testimonies those targets were not treated any differently from terrorists.
- Personnel were instructed to keep any damaging details of Palestinians' lives they came across, including information on sexual preferences, infidelities, financial problems or family illnesses that could be "used to extort/blackmail the person and turn them into a collaborator".
- Former members claim some intelligence gathered by the unit was not collected in the service of the Israeli state but in pursuit of the "agendas" of individual Israeli politicians. In one incident, for which no details have been provided, one signatory recalls: "Regarding one project in particular, many of us were shocked as we were exposed to it. Clearly it was not something we as soldiers were supposed to do. The information was almost directly transferred to political players and not to other sections of the security system."
- Unit members swapped intercepts they gathered involving "sex talk" for their own entertainment.

According to some of the 43 interviewed by the *Guardian*:

there were in effect "no rules" governing which Palestinians could be targeted and that the only restraint on their intelligence gathering in the occupied territories was "resources".

"In intelligence – in Israel intelligence regarding Palestinians – they don't really have rights," said Nadav, 26, a sergeant, who is now a philosophy and literature student in Tel Aviv. "Nobody asks that question. It's not [like] Israeli citizens, where if you want to gather information about them you need to go to court."

He said: "The intelligence gathering about Palestinians is not clean. When you rule a population that does not have political rights, laws like we have, [then] the nature of this

> regime of ruling over people, especially when you do it for many years, [is that] it forces you to take control or infiltrate every aspect of their life."

This offline mass surveillance has since increased, in particular in response to the wave of "lone wolf" attacks on Israeli soldiers and civilians in 2015-16. In 2018, the Israeli army was reported to be collecting personal information on West Bank Palestinians ubiquitously and methodically:[120]

> The army a few months ago began collecting the personal details of West Bank Palestinians, as part of its surveillance of public spaces. To this end, soldiers conduct patrols and set up temporary checkpoints. Young men who pass through are required to fill out a form. Those who are required to fill out a form must report their name, age, telephone number, identification number, type of vehicle and license number, as well as submitting a photocopy of their ID and giving both the origin and destination of the trip that brought them to the checkpoint. Women, children and old people are exempt from the form.
>
> The checkpoints operate in the early morning, when large numbers of Palestinians are on the way to work, further exacerbating the usual rush-hour traffic jams. The soldiers at each checkpoint must submit at least 100 completed forms for each shift, while the quota for the foot patrols is 30.

The army explained that the details were being entered into a Big Data anti-terrorism database, in the hope "that the information, from randomly selected individuals, can be used to foil terror attacks and to help the security forces to operate after such attacks."[121]

Later that year, it was reported that facial recognition software had been added to the CCTV cameras monitoring 27 checkpoints and that "new identification and inspection stations ha[d] been added".[122] According to Haaretz:[123]

> The Israeli surveillance operation in the West Bank is undoubtedly among the largest of its kind in the world. It includes monitoring the media, social media and the population as a whole — and now it turns out also the biometric signature of West Bank Palestinians. This monitoring op is now competing with the Chinese regime, that intensively uses facial recognition and monitors its civilians' activity on social networks.

---

120 *Israeli Army Erects West Bank Checkpoints to Collect Palestinians' Personal Details*, Haaretz, 07 March 2018, available at: https://www.haaretz.com/israel-news/.premium-idf-demanding-palestinians-personal-details-at-west-bank-checpoints-1.5883906

121 *Israeli Army Setting Up Extensive Database With Personal Details of Palestinians Collected at Checkpoints*, Haaretz, 08 March 2018 (a follow-up report to the one mentioned in the previous footnote), available at: https://www.haaretz.com/israel-news/.premium-idf-info-we-collect-on-palestinians-meant-for-anti-terror-database-1.5886616

122 *This Israeli Face-recognition Startup Is Secretly Tracking Palestinians*, Haaretz, 15 july 2018, available at: https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359

123 *Idem*.

The new, ubiquitous surveillance appears to have been a response to the shift in the West Bank Palestinian population away from organised attacks on Israeli soldiers and civilians, to "lone wolf" attacks by (especially) young Palestinians with no "known" previous links to organised groups.[124]

Apart from surveillance at checkpoints through questionnaires and facial recognition, as described above, it also involved close monitoring of online social media, in particular Facebook; and the different actions (offline and online) were increasingly coordinated. Haaretz quotes from an article co-authored by Arik Brabbing, who headed the Shin Bet's Cyber Directorate before the above-mentioned shift began, and who, as this unfolded, was named the organization's commander for Jerusalem and the West Bank, in the IDF journal Bein Haktavim, as follows:[125]

> The Shin Bet, Brabbing writes, "redirected its resources and sensors. The service planned and developed new technological, operational and intelligence tools of mining, extracting and fusing information from the internet. Immediately afterward, this was passed on for use by the end units."
>
> To fuse the information quickly – in some cases the security forces had only minutes to respond after the posting of a "Facebook last will" – cooperation with the other security branches was tightened, particularly with the IDF's Central Command and the Unit 8200 signal intelligence corps.
>
> "Military Intelligence's knowledge infrastructure for covering the population in [the West Bank] forged multiple information layers that enabled cross-checking between many identifying details. The Shin Bet's infrastructure was directed toward creating content files on entities (people, computers, houses) …. **The service's traditional expertise and knowledge of the field went hand in hand with the technological expertise of personnel in the information systems, analysis and Big Data people**."

The latter comment in particular, with its reference to data mining technologies, clearly indicates that at least in the OPT, Unit 8200 is involved in data interception and -analysis activities similar to those carried out by the USA's National Security Agency (NSA) and the UK's General Communications Headquarter (GCHQ), as exposed by Edward Snowden.[126] In fact, as noted in sub-section ii, above, Unit 8200 works directly with the NSA in this.

In that regard, it is also important to note that the Israeli security agencies also have sweeping access to online and mobile communications infrastructure in both Israel proper and the OTs.

---

124 *Idem*.

125 *Idem*, emphasis added The original article by Eric 'Harris' Berbing and Cpt. Or Glik, *The Shin Bet's Handling of Lone Wolf Terrorism*, is available at: https://www.idf.il/en/minisites/dado-center/vol-22-23-routine-security-the-campaign-between-the-wars-part-c/the-shin-bets-handling-of-lone-wolf-terrorism/

126 See sub-section ii, above. For a description of the joint US and UK surveillance activities and technologies, see Douwe Korff and Ian Brown, The inadequacy of UK data protection law in general, Part Two, *UK surveillance* (footnote 115, above), section 2.

Particularly important in that regard is the fact that although:[127]

> Palestinians have their own telecom, PalTel, which provides landline, mobile, internet, and a handful of other communication services through itself and its subsidiaries, all of which are run by Palestinians and based in Ramallah … –
>
> [in fact], all phone calls, mobile connections, and internet traffic in Palestine remain heavily dependent on Israeli infrastructure. All routing switches, cell towers, and gateway switches that PalTel uses are located in Israeli-controlled territory. This means that when a resident of Gaza calls her next-door neighbor, the call is routed through infrastructure in Israel. The same is true of mobile and internet traffic. Hadara, a Palestinian ISP owned by PalTel, doesn't have the capacity to connect directly to the web—rather, they rely exclusively on bandwidth bought from an Israeli ISP.

Presumably, much of the mobile and Internet communications of Israeli settlements are also handled by communication- and Internet service providers (CSPs and ISPs) located in Israel proper – i.e., by companies that are subject to the Israeli surveillance laws described at iv, below – and also routed through Israeli infrastructure.

Furthermore, as also noted at iv, below, the security agencies' access to the mobile phone- and Internet data infrastructure is largely unregulated in Israeli law, there is no general ban on bulk collection of communications, and such regulation as there may be is secret. Moreover:[128]

> **[T]he territorial application of Israeli online surveillance laws has not yet been regulated. Thus, the question remains of what is permitted or prohibited with respect to communications beyond the borders of the State of Israel, including in the Occupied Territories under Israel's control.**

In other words, there are no clear, specific and in their application foreseeable rules on what kinds of surveillance activities and steps – data access, data retention, data filtering and data analysis – the Israeli authorities (including Unit 8200) are allowed to carry out in the OPT, what substantive limits (if any) there are on such activities, or what kind of supervision and control there is over such activities – and there are in effect no available legal remedies that the population of the OPT can have access to in order to challenge excessive, "generalised and indiscriminate" – i.e., disproportionate – surveillance. This means that the mass surveillance in the OPT is arbitrary and in breach of international human rights- and humanitarian law.[129]

---

127 *Beyond Walls and Checkpoints: The Digital Occupation of Palestine*, Tikkun, 30 September 2014, available at: https://www.tikkun.org/beyond-walls-and-checkpoints-the-digital-occupation-of-palestine

128 Amir Cahane and Yuval Shany, Regulation of Online Surveillance in Israeli Law and Comparative Law, The Israeli Democracy Institute, Policy Paper 123, Abstract, January 2019, p. v, emphasis added, available at: https://en.idi.org.il/media/13042/regulation-of-online-surveillance-final.pdf

129 Benjamin G. Waters, An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories, Georgetown International Law Journal, 2019, available at: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2019/10/GT-GJIL190033.pdf (Written in response to the practices exposed in the letter discussed in the text)

**More specifically:**

**The surveillance in the OPT is manifestly incompatible with general international, but also especially specifically European and EU fundamental rights standards.**

In sum:

- Mass surveillance of the entire Palestinian population of the OPT except East Jerusalem, offline and online, is ubiquitous, devoid of remedies and happening outside of any clearly defined legal framework – i.e., it is arbitrary; and
- The routing of mobile and online communications between individuals in the EU and entities and individuals in the OPT through Israel proper involves "onward transfers" of the data on the EU individuals from Israel to the OPT by the Israeli providers involved.

### iv. Surveillance in Israel proper[130]

It should be clear from sub-section ii, above, that the Israeli security and defence agencies, including Unit 8200, have very far-reaching capabilities that allow them to access mobile and Internet communications including social media exchanges indiscriminately.

The extent to which they use these capabilities in Israel proper – or whether they use more limited ways of intrusion there – is unclear. Perhaps the agencies are more hesitant to use their full technical skills also in the monitoring of Israeli citizens. Or perhaps they have avoided exposure in that regard.[131]

---

130 I have no specific information on the situation in East Jerusalem or the Golan Heights, but assume that (since Israeli law is generally extended to that territory and applied there in the same way as in Israel proper: see section 5, below), the legal regimes for surveillance will also be essentially the same. Beyond this assumption, this issue is not further explored in this sub-section.

131 According to a 2015 magazine report, some years before then, "*[The Israeli Defence Force] contracted the services of Israeli tech companies to monitor both open and private posts by Israeli citizens on social media*", in particular about "protests in Hebrew on Facebook, WhatsApp, private chats and other networks, as well as data on users who write in Arabic and use words like "the Zionist state" and "Al-Quds" (Jerusalem in Arabic)." The magazine quoted a former employee as reporting that the "several of the monitoring companies create fictitious profiles as a tracking technique. These profiles connect with specific individuals that the system wants to monitor. This is how the companies 'circumvent' privacy mechanisms, so that even when a user marks a specific piece of content as private (intended for his/her friends alone), the companies still have access to it and are able to pass it on to the security services." See: *Exclusive: The IDF is monitoring what Israeli citizens say on Facebook*, +972 Magazine, 15 July 2015, emphasis added, available at:
https://www.972mag.com/the-idf-is-monitoring-what-israeli-citizens-say-on-facebook/
But in fact, as detailed above, it appears that Unit 8200 at least now uses much more advanced "hacking" and "tapping into" of the communication cables technologies, similar to the US NSA and the UK GCHQ. Perhaps these newer technologies were only adopted by the IDF after the article – or the authors of the article (which focussed on the intrusion of the privacy of Israelis) were unaware of the advanced measures.

Either way, it should be noted that the legal framework – such as it is – is clearly seriously deficient. It is usefully briefly summarised in a 2019 paper by the Israeli Democracy Institute (already alluded to), from which the following excerpts must here suffice: [132]

> Examination of Israeli legislation applying to online surveillance of communication networks shows that Israeli law suffers from under-regulation of a series of issues … For example, **Israeli law has no general ban on bulk collection of communications, not even a ban coupled with provisions for exceptional cases** in which such activity would be permitted, subject to criteria of proportionality and absolute need. …
>
> In addition**, there are no provisions in Israeli law with respect to temporal limitations on the retention of communications data by communications providers** ... This refers both to the communications content itself and to metadata, which consist of information about the communication other than its content, and from which (among other things) details of the parties to the communication, and of where and when it occurred, can be ascertained.
>
> Similarly, **data-mining activities** carried out in this context—that is, using statistical techniques to analyze databases obtained by means of online surveillance, including cross-referencing them with other government databases—**are barely addressed in Israeli legislation** …
>
> …
>
> Current Israeli legislation affords the government broad discretion in setting **rules to regulate the Israel Security Agency's (the ISA or General Security Service) surveillance of communications networks, and to regulate the orders issued to telecommunication licensees** (licensed to provide telecommunications services including telephony, internet, and cellular services) to assist the security forces (including the Israel Police). These rules, and a portion of the parliamentary and administrative oversight thereof and of online surveillance practices, **are kept secret**.
>
> **[J]udicial review of various authorizations for online surveillance is limited in scope.** The law absolves security agencies seeking a wiretapping order from applying to the courts and settles for a permit granted in advance by the minister responsible; in urgent cases, retroactive ministerial authorization is allowed, as long as the use of these powers is reported to the attorney general.
>
> …

---

[132] Amir Cahane and Yuval Shany, Regulation of Online Surveillance in Israeli Law and Comparative Law (footnote 128, above), pp. v – vi, emphases added.
For a more detailed legal analysis, with full references, see: Omer Tene, *Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability*. Excerpts from this paper, relevant to the present opinion (and this sub-section) are provided in an annex to this sub-section.
For earlier studies, see, e.g.: Andrew Stephens, Surveillance Policies, Practices and Technologies in Israel and the Occupied Palestinian Territories: Assessing the Security State, The New Transparency, Working Paper IV, November 2011, available at: https://www.sscqueens.org/sites/sscqueens.org/files/2011-11-Stevens-WPIV_0.pdf
This drew *inter alia* on Usama Halabi, *Legal analysis and critique of some surveillance methods used by Israel*, in: E. Zureik, D. Lyon and Y. Abu-Laban (eds), Surveillance and Control in Israel/Palestine, 2011 (not available online).

> **Collection of communications data by the ISA (via direct interception, online access, or occasional request) is not subject to any judicial authorization.** Moreover, the applicable legal provisions may be interpreted so that the mere collection of communications data does not require authorization from the head of the ISA, and such authorization is only necessary for using of the acquired information.
>
> …
>
> Judicial and quasi-judicial review of surveillance of communication networks is reactive, and its response is limited to specific applications or orders. This kind of oversight does not address cases in which the authorities avoided applying for the relevant orders due to the absence of a legal obligation to do so or due to a narrow interpretation of the existing statutory obligations. …
>
> In Israel, **the Privacy Protection Authority** (formerly the Israel Law and Technology Authority—ILTA) is the regulatory, supervisory, and enforcement body under the Protection of Privacy Law, the Credit Data Law, and the Electronic Signature Law. However, due to exemptions in the Protection of Privacy Law, the Authority **does not, in practice, oversee the online surveillance activity of security and law enforcement agencies**.
>
> …
>
> Currently, the scope of the Knesset's parliamentary review of police and Israel Security Agency online surveillance practices is restricted to statutory reports pursuant to the Wiretap Act, some of which are delivered behind closed doors. Similar reports under the provisions of the Communications Data Act were submitted for a limited period by virtue of a temporary provision in the law, which has since expired. An attempt to obtain these secret reports through a request under the Freedom of Information Law was rejected by the Supreme Court which, in a side comment, recommended that the state disclose these details voluntarily and before they are leaked, in order to secure public trust.

It is clear from the above, and especially from the more in-depth summaries of the law in Tene's paper,[133] that:

- **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.**

133 See previous footnote.

This is 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.

**Concerns about the use and possible abuse of the surveillance powers in relation to the Corona virus pandemic:**

Specific concerns have been raised about the use of the above powers in relation to the current Corona virus pandemic. Under an arrangement that was originally not based on any law but has since been given such a basis (see below):[134]

> the ministry of Health hands over the details of patients who tested positive to Covid-19 to Shin Bet and Shin Bet gives them back a list of every person they have been in contact with over the past 2 weeks. Being 'in contact' is defined as spending a minimum of 15 minutes within 2 meters of the infected person. The people on that list then receive a text message requesting them to go into isolation, meaning they have to stay home and are not allowed to go out under any circumstance.

On the legal situation in this regard, *Privacy International* reports as follows:[135]

> Initially, the measure was pushed through by Prime Minister Benjamin Netanyahu, as Israel – with no government for over a year – was at the time undergoing a democratic crisis on top of the health crisis. But an appeal made by the Association for Civil Rights in Israel (ACRI), the Adalah Legal Center for Arab Minority Rights and the Arab Joint List led the High Court to assert that such a measure would need to be scrutinised by a parliamentary committee, without the formation of such a committee, the tracking would have to be stopped.
>
> The parliamentary committee was eventually formed and the tracking of the population has been pursued. The government's decision to rely on Shin Bet for the tracking, however, was still being challenged at the High Court by ACRI, Adalah and the Union of Journalists in Israel.
>
> A decision was reached on April 26th [2020], as the High Court decided that the government would need to pass a new legislation in order to be able to carry on relying on Shin Bet for the surveillance of Covid-19 patients. The ruling states:
>
> > The choice to make use of the state's preventative security agency to follow those who do not seek to do [the state] harm, without the subjects of the surveillance giving their permission, raises an extremely serious difficulty and a

---

134 Privacy International, *Israel's coronavirus surveillance is an example for others - of what not to do*, 1 May 2020, available at: https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do

135 *Idem*.

> suitable alternative should be sought that fulfils the principles of privacy protection.

The Israeli choice of using its national security service to tackle the pandemic has been criticised as:[136]

> an extreme approach that is at odds with other democracies, constitutes an unprecedented privacy violation, and lays the groundwork for invasive surveillance tools to be used in applications besides public health.

Here, it will suffice to note that this episode underlines the very broad and detailed access that the Israeli security agencies have to the communications data and devices, including the location data relating to those devices, of anyone in Israel proper (as well as in the OTs) – and how easily such powers can be abused or mis-used.

[136] Tehilla Shwartz Altshuler and Rachel Aridor Hershkowitz, *How Israel's COVID-19 mass surveillance operation works*, 6 July 2020, available at: https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/

## ANNEX TO SECTION 4.2.4, SUB-SECTION IV – Surveillance in Israel proper

**EXCERPTS FROM:** Omer Tene, Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability, 2017[137]

**NB: The descriptions in the text below only refer to the law in Israel proper; they do not cover the law or situation in the Occupied Palestinian Territories (OPTs). Also, whereas Tene generally covers, under each of his headings, both law enforcement and national security agencies' powers and procedures, the excerpts below are generally limited to his descriptions of these issues in relation to national security.**

As Tene notes:[138]

> Section 19 of the [PPA] provides an exemption from liability under Section 2 for "security services," defined to include the police, military intelligence (known according to its Hebrew acronym "Aman"), the Israeli Security Agency (ISA) (known according to its Hebrew acronym as "Shin Bet" or "Sahabak"),[139] and the Institute for Intelligence and Special Operations (known according to a shorthand version of its Hebrew name, "Mossad").[140] It states:
>
> (a) No person shall bear responsibility under this Act for an act which he is empowered to do by law.
>
> (b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Act for an infringement reasonably committed within the scope of their functions and for the purpose of carrying them out.
>
> Nongovernment entities cooperating with a security service while compromising the privacy interests of their customers can rely for a defense on Section 19(a) above as well as on Section 18(2)(b) of the [PPA], which states that "[i]n any criminal or civil proceeding for infringement of privacy, it shall be a good defence if (…) (2) the defendant or accused committed the infringement in good faith and in any of the following circumstances: (b) the infringement was committed in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit it."

He adds the following specifics on government access to data:[141]

> **A. Facilitating Government Surveillance**
>
> Similar to the Communications Assistance for Law Enforcement Act (CALEA) in the United States, Section 13 of the Israeli Telecommunications Act (Telephone and Broadcast), 1982 (Telecommunications Act) empowers government officials to provide instructions to

---

137 Full reference: Omer Tene, *Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability*, Chapter 4 in: Fred H. Cate and James X. Dempsey (eds.), Bulk Collection: Systematic Government Access to Private-Sector Data, Oxford Scholarship Online, October 2017, available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-4

138 P. 95.

139 The ISA is responsible for internal security, domestic intelligence and counter- intelligence, and the fight against terrorism. [original footnote]

140 The Mossad is responsible for foreign intelligence and covert missions beyond Israel's borders. [original footnote]

141 Pp. 96 – 98, emphases in the text added

telecommunications operators to modify and design their equipment, facilities, and services to ensure that they have built- in surveillance capabilities. [I.e., to install so-called **"back doors"** – DK][142]

Under Section 13 of the Telecommunications Act, the prime minister, after consulting with the Minister of Communications and based on a request by the Minister of Defence, Minister of Domestic Security, the ISA, or the Mossad, can issue instructions to a telecommunications licensee with respect to "the installation of equipment, performance of a telecommunications service, or ensuring technological compatibility to telecommunications equipment (…) including the provision of access to equipment, as much as necessary to perform the roles of the security services or exercise their legal authority."[143] Section 13(a) of the Telecommunications Act defines a "security service" to include the Israel Defence Forces, ISA, Mossad, police, and prison service. A licensee is defined broadly through a complex set of definitions in Section 1 of the Telecommunications Act30 to include any fixed line or cellular operator, and ISPs, as well as broadcast licensees (cable and satellite operators).

Under Section 13(d) of the Telecommunications Act, **the prime minister's instructions under Section 13(b) must remain secret.** Section 13(e) of the Telecommunications Act provides immunity from civil or criminal liability (for example, for infringement of privacy) to a licensee and its employees for complying with an obligation under the same section. …

…

**B. Wiretapping**

Wiretapping, or lawful intercept, is regulated in Israel under the Wiretap Act, 1979 (Wiretap Act). The Wiretap Act generally prohibits wiretapping and sets rules for lawful intercept by law enforcement and national security agencies.

…

Lawful intercept by the police is allowed pursuant to a warrant issued by a President of a District Court.[144] A broader mandate is provided to security services, defined as military intelligence or the ISA. **A security service may obtain a permit for a wiretap from the prime minister or the Minister of Defence (in this Act, the "Minister") without judicial oversight.** Under Section 4 of the Wiretap Act, "the Minister may authorise a wiretap in writing if requested to do so in writing by the head of a security service and if he is convinced, after giving due weight to the infringement of privacy, that it is necessary for national security." Sections 4(b)– (c) of the Wiretap Act describe the specifics that must be found in a Minister's permit, including the identity of the individual or device whose communications will be

---

142 The technical specifications of the "pipes" are contained in annexes to the e-communication service providers' licences, which are secret. See "*The Mechanics of Data transfers*" (here meaning disclosures of data by e-communication service providers to the authorities), at p. 107. The legality of this secrecy was confirmed by the courts in the *Amir Liran v. Pelephone* case (Civ. 1994/06 Amir Liran v. Pelephone (Tel Aviv District Ct. November 30, 2010)), also discussed by Tee on p. 107.

143 Telecommunications Act (Telephone and Broadcast), 1982, § 13(b)(2). [original footnote]

144 A president of a District Court in Israel is a senior judge who ranks junior to only Supreme Court justices. [original footnote]

> intercepted, the location of the conversations, and the duration of the monitoring (not to exceed three months, subject to periodic extension). However, the requirement to specify such details is qualified by the phrase "all if they are known in advance." **This implies that the Minister may well issue general wiretapping permits** [i.e., wiretapping permits covering whole groups or categories of individuals – as are also used in other countries, such as the UK – DK]. In urgent cases, the head of a security service may himself authorize a wiretap for a period no longer than 48 hours; immediate notice must be sent to the Minister who is authorized to revoke such a wiretap.[145]
>
> Although not subject to judicial oversight, national security wiretap permits are reported quarterly to the attorney general;[146] and the number of such permits is reported annually to a special parliamentary committee convening behind closed doors.[147]

Tene notes that "[i]n the past few years, two high level inquiries were conducted into police … use of wiretapping, one by a parliamentary committee and the other by the State Comptroller" – but also that no such inquiry has ever been held into wiretapping by the national security agencies.[148]

> **C. Communications Data**
>
> … [A]ccess by the ISA [intelligence agencies] to communications data is regulated by a specific provision in **the General Security Service Act, 2002 (ISAA). … which confers far broader powers to the ISA [than are accorded to the law enforcement agencies** under the highly contested 2007 (Communications Data Act)][149] and does so **without any judicial scrutiny**.
>
> …
>
> - **Security Services Access**
>
> [T]he ISA enjoyed broad access to communications data even before the enactment of the Communications Data Act. In the 1990s, the government of Israel decided to enact a law regulating the status and powers of the ISA, which until then operated based on government decisions and without legislative mandate.[150] Years of preparatory work by the legal department of the ISA and the Ministry of Justice led to the enactment of the ISAA in 2002.[151] The ISAA treads a middle path between "skeletal" national security agency statutes,

---

145 The Wiretap Act, § 5. [original footnote]

146 The Wiretap Act, § 4(d). [original footnote]

147 The Wiretap Act, § 4(e). [original footnote]

148 P. 99. The text quoted under the headings "Communication Data" and "Data Retention" come from pp. 100 – 107. Emphases in bold in the text again added.

149 For details of the challenges to the Communications Data Act, see p. 100.

150 The decision to legislate was motivated by a series of public scandals, such as the execution without trial of two Palestinian terrorists by ISA operatives and later attempt of cover- up (the "Line 300 Scandal"); as well as the Supreme Court decision in the Public Committee Against Torture case, supra note 4, outlawing the use of force in interrogations. [original footnote]

151 For a thorough review of the legislative process and rationale see Arye Rotter, The General Security Service Act— Anatomy of Legislation, Mar. 2010. (Rotter was Legal Counsel for the ISA during the legislative process). [original footnote]

such as the UK's,[152] and voluminous, detailed statutes, such as Australia's.[153] Although not addressing thorny issues such as the use of force in interrogations, the ISAA does introduce a specific section for communications data[, Section 11].[154]

…

**Section 11(b) grants the prime minister almost unfettered authority to promulgate rules setting forth categories of communications data that a licensee[155] must transfer to the ISA.** Such rules were in fact put in place by the prime minister, yet **their content remains classified** in accordance with Section 19(a)(1) of the ISA.69 Under Section 11(c) of the ISAA, the Head of the ISA has broad powers to permit ISA access to or use of such categories of communications data that the prime minister set forth in his rules. Indeed, the only condition qualifying both the prime minister's and Head of ISA's respective authority is that the communications data "are required for the ISA for performing its roles under this law." The communications data subject to the ISA authority include any data held by a licensee with the notable exception of communications contents.[156]

To counterbalance these broad powers, the ISAA sets forth **certain transparency requirements**. First, under Section 11(c) of the ISAA, the Head of ISA must specify in each permit details concerning the data sought, the purpose for which they are sought, and the database in which they are found. Yet this requirement is tempered by the modifier "inasmuch as possible," **effectively allowing for much less detailed permits**. In addition, each permit is limited in duration for a period no longer than six months; yet such a term **may be extended time and again indefinitely**. More significant, under Section 11(d) of the ISAA, the Head of ISA must **report periodically** to the prime minister and the attorney general (quarterly) and to the parliamentary committee for ISA matters (annually) about permits issued and data used under Section 11. [However, **t]hese reporting requirements [are] not public or subject to judicial oversight**.[157]

The final provision of Section 11 of the ISAA provides immunity from civil or criminal liability to a licensee and its employees for complying with an obligation under the same section. …

Finally, it is important to note that access to communications data for national security purposes under the ISAA is restricted to the ISA; the regime does not apply to additional national security organizations such as the Mossad and Aman, particularly Unit 8200 responsible for SIGINT (signals intelligence).[158] **There is no public information concerning these organizations' access to domestic communications data, if any.**

---

152 Security Service Act 1989, c. 5, which has only seven sections. [original footnote]

153 Australian Security Intelligence Organisation Act 1979, Act No. 113 of 1979. [original footnote]

154 General Security Service Act, § 11. [original footnote] Section 11 is quoted in full at pp. 103 – 104.

155 A licensee is defined broadly in the Telecommunications Act to include any fixed line or cellular operator, and ISPs, as well as broadcast licensees (cable and satellite operators). See Tene, footnote 30.

156 See definition of "Data;" General Security Service Act, § 11(a), which stands in stark contrast to the highly detailed and nuanced definition of communications data in the Communications Data Act. [original footnote]

157 Tene feels these reporting requirements are still "significant, as they are made to the highest official in the executive branch (the prime minister) and the legal service (the attorney general), as well as to the legislative branch (the parliamentary committee)", and emphasises the special constitutional role of the A-G.) Pp. 105 – 106.

158 See, for example, Gil Kerbs, "*The Unit*," Forbes, February 8, 2007,

**D. Data Retention[159]**

> Unlike the EU,[160] Israel does not have a general data retention statute. This means that the telecom operators could ostensibly delete communications data promptly after using them for their own purposes. Indeed, one interpretation of the purpose limitation provisions in the [PPA][161] is that such deletion is required by privacy law. To this end, **Section 11(e) of the ISAA authorizes the prime minister to promulgate rules "regarding the retention by a licensee[162] of categories of data according to subsection (b), for a period that he determines." As discussed, such rules, if they have been put in place, remain secret.** A similar provision is not found in the Communications Data Act, raising doubts whether telecom operators must retain data if not required to do so by the prime minister's national security rules.[163]

Tene also mentions the establishment, in 2015, of the National Cyber Defence Authority which was given a broad brief that includes:[164]

> Conduct[ing], operat[ing], and implement[ing], as needed, all the operational defensive efforts in cyberspace at the national level, including handling cyber threats and incidents in real time, formulating an ongoing situational awareness, consolidating and analyzing intelligence, and working with the defense community as detailed in a classified addendum; [and] operat[ing] the national Cyber Event Readiness Team (CERT)

He adds that:[165]

> At this point, it remains to be seen what if any voluntary or obligatory data sharing requirements will be imposed on businesses vis-à-vis the Authority or national CERT.

Finally, he mentions the following "additional laws", with a comment in the last sentence:[166]

> In addition to the laws discussed above, which focus on communications data, Israel has launched various legislative initiatives involving collection of personal data by government, including a national biometric database (Law on Inclusion of Biometric Identifiers in Identification Documents and Database, 2009), a new credit reporting database (Credit Information Act, 2016), a connected cities initiative (City Without Violence), and **a government decision to access to PNR and API (Advance Passenger Information) data of**

---

http://www.forbes.com/2007/02/07/israel-military-unit-ventures-biz-cx_gk_0208israel.html. [original footnote]

159 In Tene's chapter, this heading is numbered "3" (p. 106).

160 Directive 2006/24/EC of the European Parliament and of the Council of 15 Mar. 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 (April 13, 2006). [original footnote] Note that this directive ("the Data Retention Directive") was invalidated by the Court of Justice in the EU.

161 Privacy Protection Act, §§ 2(9) and 8(b). [original footnote]

162 As broadly defined: see footnote 155, above.

163 See the discussion of the *Amir Liran v. Pelephone Case* on p. 107 (see footnote 142, above).

164 P. 109.

165 *Idem*.

166 *Idem*.

**airlines flying to and from Israel (Government of Israel Decision 2258)**. These laws and initiatives demonstrate an ongoing erosion in privacy protections for individuals' data, particularly when faced with strong state interests.

I should add that state demands for access to PNR and API data is controversial in Europe,[167] with the EU PNR Directive[168] being challenged in the CJEU.[169]

- o – O – o -

[167] See Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, Council of Europe, 2015, available at: https://rm.coe.int/16806a601b

[168] Directive (EU) 2016/681 of the European Parliament and of The Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016, p. 132ff, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0681&from=DE

[169] See EDRi/Gesellschaft für Freiheitsrechte, *CJEU to decide on processing of passenger data under PNR Directive*, 29 January 2020, available at: https://edri.org/cjeu-to-decide-on-processing-of-passenger-data-under-pnr-directive/

## v. Surveillance of foreigners and their communications

The +972 Magazine article on the IDF's monitoring of what Israeli citizens say on Facebook, mentioned in the previous sub-section, also noted that:[170]

> In 2011, the IDF established an "[anti] de-legitimization branch" as part of Unit 8200, whose stated goal is to gather **intelligence on foreign organizations that oppose Israeli policies. The branch focuses on those who criticize Israel, and specifically BDS [Boycott, Divestment, Sanctions] and flotilla activists, as well as bodies that are at the forefront of legal struggles targeting Israel, such as the International Criminal Court**. After Operative Protective Edge in 2014, the unit mainly gathered intelligence that would aid Israel in its struggle against UN reports on war crimes that allegedly took place during the war.

This is relevant in particular in relation to the *Le Monde* report, cited earlier, according to which Unit 8200 monitors the phone calls, emails, and other communications of both friendly and enemy nations across the Middle East, Europe, Asia, and Africa, including by tapping into the underseas cables that link Israel to Europe.[171]

In other words, and not really surprisingly, Israel's Unit 8200 acts just like the US's NSA and the UK's GCHQ in accessing the global communications infrastructure through which landline, email, mobile and Internet communications flow, extracting the data in bulk, before filtering and analysing it by means of both simple search terms – such as "boycott", "demonstration", "illegal occupation", etc. – and sophisticated algorithms.[172]

Significantly, this activity can be used in relation not only to communications between the EU and Israel proper (and East Jerusalem and the Golan Heights), but also in relation to communications between the EU and the OPT, because as noted earlier, all (or almost all) such communications are routed through communication- and Internet service providers (CSPs and ISPs) that are based in Israel, and thus subject to the Israeli surveillance laws and powers.

In part 6, I will discuss the implications in relation to the EU adequacy decision on Israel.

- o – O – o -

170 See footnote 131, above.
171 See footnote 107, above.
172 *Idem*.

## 4.3 Conclusion

In the light of the above, I conclude that the level of protection of personal data provided by the Israeli Privacy Protection Act (PPA) is clearly far from "essentially equivalent" to that provided by the GDPR, in all three aspects that need to be considered in an adequacy process:

- the substantive protections of the PPA fall far short of the "core" substantive requirements of EU law;
- the Privacy Protection Authority does not provide "essentially equivalent" "procedural/enforcement" protection (in particular because of its lack of real independence); and
- the Israeli authorities have excessive, indiscriminate access to personal data of individuals in both Israel proper and the OTs, including to any such data as may be transferred from the EU to Israel and/or onwardly transferred via Israel to the OTs, without there being appropriate remedies in place – and the latter includes data on EU individuals who communicate by electronic means (mobile, landline or Internet) with individuals in Israel proper or the OTs.

**In my opinion, in the circumstances, and in the light of the *Schrems* judgments in relation to the powers of the U.S. intelligence agencies and the lack of remedies against them, the EU adequacy decision on Israel therefore cannot and should not be renewed under the GDPR; rather, the 2011 adequacy decision, adopted under the 1995 Data Protection Directive and the previous, much weaker assessment criteria, should be repealed or at least suspended, with immediate effect.**

**If the Commission were to allow the 2011 decision to remain in place, or to issue a new positive adequacy decision, those could be challenged in the CJEU – and such a challenge would be most likely to succeed.**

**The implications are discussed in part 6, below, in the light of the issues of territorial application of the PPA, its provisions on onward transfers of personal data, and the EU's "differentiation policy".**

- o – O – o –

# 5. Issues of territoriality

## 5.1 Territorial application of Israeli law

### 5.1.1 Territorial application of Israeli law generally

In 1967, Israel occupied the Golan Heights, Gaza, and the West Bank including East Jerusalem. It subsequently annexed East Jerusalem and the Golan Heights by adopting acts applying Israeli "law, jurisdiction and administration" to these two areas: East Jerusalem in 1967[173] and the Golan Heights in 1981.[174] As a matter of Israeli law, these two territories form part of the State of Israel, and Israeli law applies there in principle exactly as it does in Israel.

Throughout all of the Occupied Territories (OTs), Israel also facilitated the creation of settlements of Israeli citizens.

Unlike the East Jerusalem and the Golan Heights, the West Bank has not been formally annexed. It is, in principle, subject to Israeli military law and surviving Jordanian law – which are the laws that are applied to the Palestinian inhabitants. However, although the Israeli settlements in the West Bank have not been formally annexed, Israeli law applies to them to a large extent in practice. This has been done by means of military orders applying Israeli laws to settlements within the boundaries of their local or regional councils (so-called "enclave law"), through extra-territorial application of Israeli laws on a personal basis to Israeli nationals (settlers), and through rulings of the Israeli Supreme Court (High Court of Justice).[175]

The Association for Civil Rights in Israel (ACRI) described the resulting situation in a 2014 report with a quote from Supreme Court Judge Eliezer Rivlin:[176]

> "*The Israeli residents living in the West Bank are subject to extensive parts of Israeli law, in addition to special legislation by the military commander that applies solely to the Israeli residents. The Palestinian residents living in the very same territories are subject to Jordanian*

---

173 Law and Administration Ordinance (Amendment No. 11) Law, 5727-1967.

174 Golan Heights Law, 5742-1981, 1981-1982 S.H. 6.

175 ACRI, One Rule, Two Legal Systems: Israel's Regime of Laws in the West Bank, October 2014, available at: https://law.acri.org.il/en/wp-content/uploads/2015/02/Two-Systems-of-Law-English-FINAL.pdf
See also: Human Sciences Research Council, Occupation, Colonialism, Apartheid? A re-assessment of Israel's practices in the occupied Palestinian territories under international law, 2009, pp. 105 – 113, available at: http://sro.sussex.ac.uk/id/eprint/43295/1/Occupation_Colonialism_Apartheid-FullStudy_copy.pdf

176 ACRI, One Rule, Two Legal Systems: Israel's Regime of Laws in the West Bank, October 2014, p. 5, available at: https://law.acri.org.il/en/wp-content/uploads/2015/02/Two-Systems-of-Law-English-FINAL.pdf
See also the Report of the independent international factfinding mission to investigate the implications of the Israeli settlements on the civil, political, economic, social and cultural rights of the Palestinian people throughout the Occupied Palestinian Territory, including East Jerusalem, submitted to the UN Human Rights Council, 7 February 2013, UN Document A/HRC/22/63, paras. 39 – 40, available at: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session22/A-HRC-22-63_en.pdf

> *law and to legislation by the military governor that applies to them […]* ***This outcome creates a regime in which different sets of laws apply in one territory.***"[177]

The ACRI report said this has led to "the creation and development of an official and institutionalized legal regime of two separate legal systems, on an ethnic-national basis". It added that:[178]

> **in a gradual process that stretched over four decades, the Israeli legal system was applied to settlers in the West Bank almost in its entirety, while the Palestinian residents living in the same territory remained subject to the military legal system.** The duality of laws under the Israeli rule in the West Bank has far-reaching implications with regards to the rights of the Palestinian residents and to their daily lives. **As a general rule, the military legislation they are subject to is far more severe than the Israeli legislation applied to settlers, and this discrimination touches upon almost every aspect of life.**

Since 2015, a marked shift has taken place. A number of laws have been introduced and passed in the Knesset that directly apply to West Bank settlements – rather than relying on the IDF military commander to issue an order to apply them in the West Bank. In this way, Knesset increasingly regards itself as the direct legislative authority in the West Bank.[179] As part of this political trend, new guidelines issued by Israel's Attorney General in December 2017 stipulate that all new government-sponsored bills must address the applicability of the proposed legislation to settlers in the West Bank.[180] In January 2018, the Knesset House Committee decided that Parliament's legislative committees should also address the application of each new law to settlements.[181] These developments further erase the distinction between the legal systems inside Israel proper and in settlements, while deepening the dual legal system in the West Bank.

By contrast, as noted in part 2, above, the EU and the wider international community do not recognise Israeli sovereignty over any part of the occupied territories, irrespective of their status under Israeli domestic law. Israel and the EU (and the wider international community) therefore have different, incompatible views on the question of territoriality and applicable law, as illustrated overleaf.

---

177 HCJ 5666/03 *Kav LaOved v. Jerusalem Labor Court*, 62(3) 264, para. 25 of the judgement of Justice Rivlin (2007) (hereinafter: the *Kav LaOved* case). [original footnote; the emphasis in bold in the quote is also original]

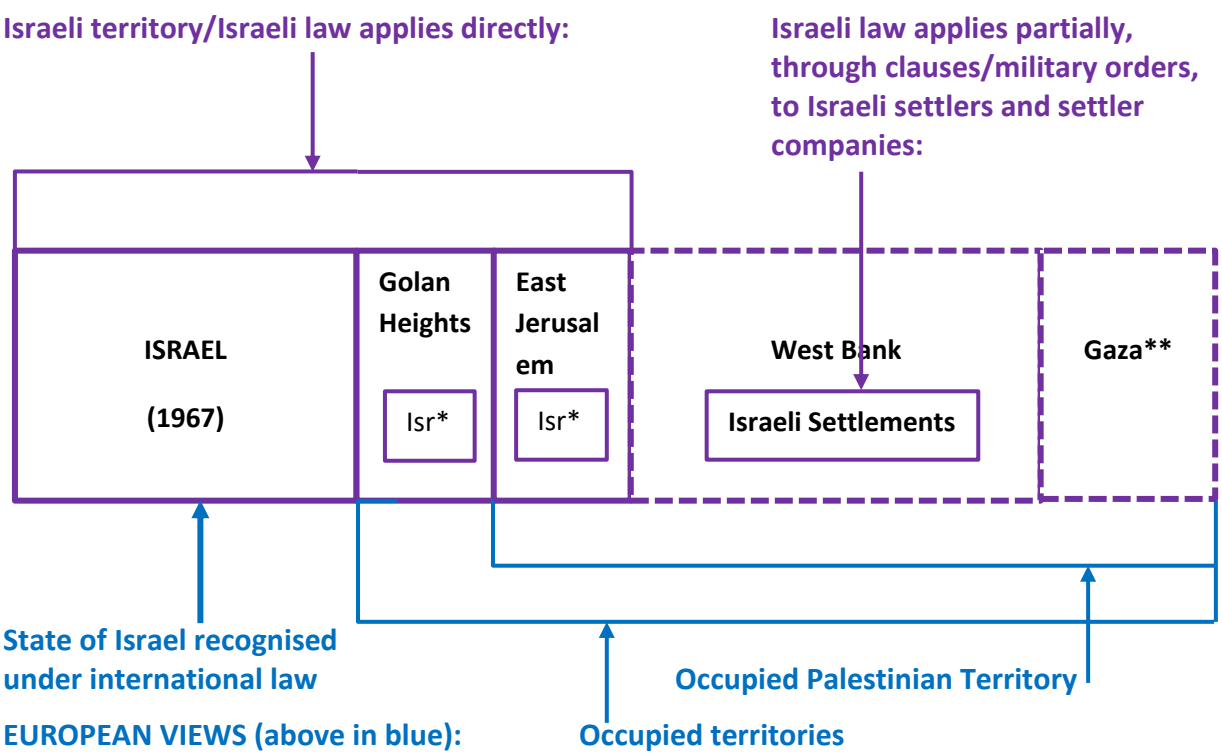
178 ACRI, One Rule, Two Legal Systems: Israel's Regime of Laws in the West Bank (footnote 175, above), p. 7, original emphases.

179 Yesh Din, Annexation Legislation Database, available at: https://www.yesh-din.org/en/about-the-database/

180 Haaretz, 31 December 2017, *New Laws Should Also Consider Settlers in West Bank, Says Israeli Attorney General*, available at: https://www.haaretz.com/israel-news/.premium-new-draft-laws-must-also-consider-settlers-in-west-bank-says-israeli-ag-1.5630121

181 Jerusalem Post, 3 January 2018, *Knesset committees to discuss applying new laws to West Bank*, available at: https://www.jpost.com/Israel-News/Knesset-committees-to-discuss-applying-new-laws-to-West-Bank-532717

**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).

### 5.1.2 Territorial application of the PPA

There is no law in Israel that defines its borders. Consequently, there is no express legal clarity of what territories are "within the state's borders" or "outside of the state's borders" (a phrase often translated as "abroad" in English translations of Israeli law).

More specifically, the Privacy Protection (Transfer of Data to Database Abroad) Regulations, 5761-2001, which specify restrictions and exceptions of personal data transfers to databases outside the borders of the state (or abroad according to the English translation) also do not define what is covered by these concepts.[182]

---

[182] Section 24 PPA stipulates that "This Law shall apply to the State", but this is presumably intended to indicate that Israeli state entities are not exempt from the law (although there are sweeping exemptions in relation to security

However, as noted in the previous section, there are specific laws that declare that East Jerusalem and the Golan Heights are part of Israel's territory and that every Israeli law is applicable in those territories, i.e.: the Golan Heights Law 5742-1981, and the Basic Law: Jerusalem.

Consequently, the PPA applies in the Golan Heights and East Jerusalem in the same way as it does in Israel proper (and there are no restrictions on transfers of personal data from Israel proper to East Jerusalem or the Golan Heights: see the next section).

In legal logic, it follows from the fact that the West Bank is not considered part of Israel, i.e., is not "within the state's borders", that the PPA does not apply there. However, it would appear that in practice, for the purposes of the PPA, individuals and companies in the settlements in the West Bank are treated in the same way as individuals and companies in Israel proper, East Jerusalem and the Golan Heights. Certainly, personal databases of companies and other entities based in Israeli settlements in the West Bank are included in the register of registerable databases maintained by the Privacy Protection Authority.[183] At least 150 databases in the register have an address in the settlements. The Annex to this section provides a number of selected examples.[184]

By contrast, it would appear clear that the PPA does not apply in law, and is not applied in practice, to processing of personal data by Palestinian individuals, companies or public bodies in the West Bank outside the Israeli settlements there (and that any transfer of personal data from Israel proper to such individuals, companies or public bodies *are* regarded as transfers "abroad" in terms of the PPA: see yet again the next section).

---

agencies: see sections 19 and 20). It does not appear to mean "This Law shall apply to entities within [the borders of] the State".

[183] The link to the database is here:
https://data.gov.il/dataset/23dbaf64-b284-4c59-8b11-b7fc6f1a9ecf/resource/fd56bf5b-7918-4906-99e4-b0e5102ae268/download/pinkas_list_hofesh_hameida.csv
As noted in section 3.1, above, the PPA is based on a system of registration of databases: the Law applies to possessors of registered databases – i.e., in practice, in the private sector, to companies that hold such collections of data and use the data for commercial purposes. The register is maintained by the Israeli Privacy Protection Authority (originally named the Registrar of Databases). Under section 9 PPA, an application for registration of a database must contain the following information that is of relevance here:

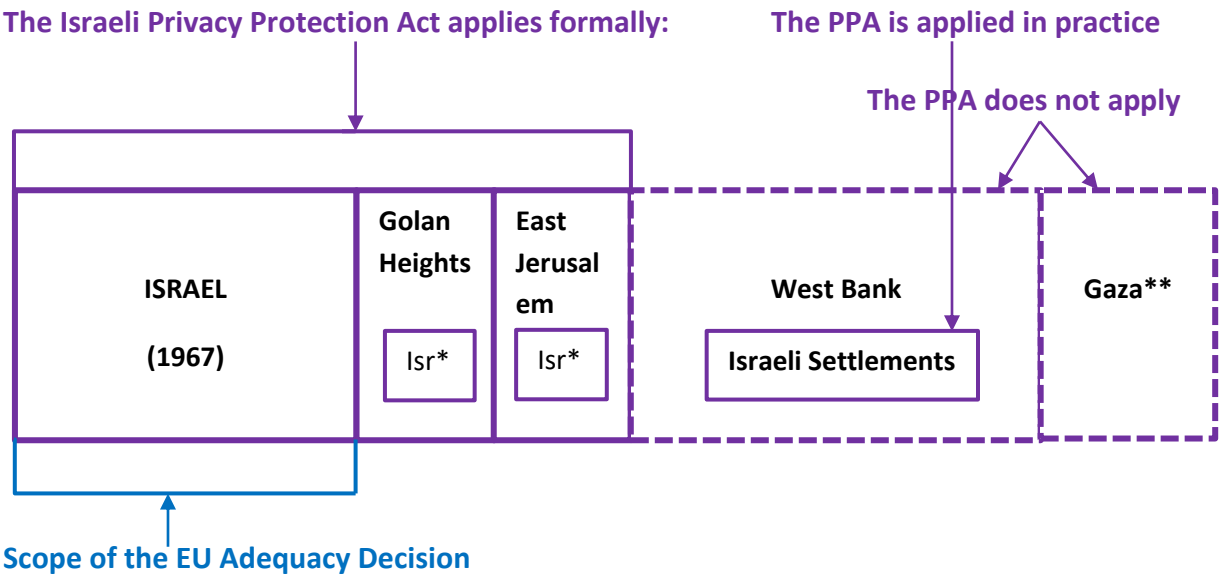
- the names of the owner of the database, the possessor of the database and the manager of the database, and their addresses in Israel; and
- particulars on the transfer of information abroad.*
  * in other translations and summaries of the Law, this reads: "details regarding transfers of data outside the borders of the state"

Section 3 PPA defines "possessor, for the purpose of a database" as "a person who has a database in his possession permanently and is permitted to use it". A database is essentially any collection of certain listed personal data that are processed by automatic means, except for collections that are "not for business purposes" or that only contain contact details of individuals (section 7).

[184] From those, it would appear that the register is rather sloppily maintained: a significant number of supposedly mandatory details are simply omitted; several entries appear very old (without it being clarified if they have been updated or renewed at any time, or when); and the status of several of them is given as "Debt suspended" – which presumably means the relevant fees have not been paid. See also the notes under the Annex. But I will not examine that issue here further.

In chart form:

**Chart 2:** **The territorial application of the PPA**



## ANNEX TO SECTION 5.1.2 – Territorial application of the PPA Surveillance in Israel proper

**Extracts from the register of registerable databases maintained by the Privacy Protection Authority (Edited examples):**[1] (See notes under the extracts)

**Legend**:

Dbase = database - = no entry in register Israeli settlements in the West Bank in **red**

| **Dbase Nr./ Dbase ID/ Registrn date** | **Name of dbase holder** | **Name of dbase** | **City (or settlement) Area Code/[2] Country/ State** | **Data sent abroad?** | **Dbase status** |
|---|---|---|---|---|---|
| 113784<br>580367290<br>10/03/2013 | Ariel University in Samaria | Student & worker administration | **Ariel**<br>-<br>-<br>- | | Approved |
| 159102<br>511984213<br>20/01/2003 | Tzifcha International 1994 LTD | "No name" | **Modi 'in Illit**<br>**7183402**<br>-<br>- | No | Approved |
| 362832<br>51158909<br>13/11/2001 | Delta Construction Ltd | Index of buyers | **Oranit**<br>**4481300** | No | Debt suspended[3] |
| 1091068<br>51177118<br>- | T.G. Biotechnological Institutes Ltd | Database of hospitalized patients (in Hod Adumim) | **Ma'ale Adumim**<br>**9842108**<br>**Israel**[4] | No | Debt suspended[3] |
| 880000228<br>550003230<br>24/10/2004 | Elazar Data Processing | Accounting and resource management | **Gush Etzion**<br>**90942**<br>-<br>- | No | Debt suspended[3] |
| 980022618<br>500104633<br>- | Ministry of Defense / DCO of Judea and Samaria | Health insurance in Judea and Samaria | **Beit El**<br>**9063101**<br>- | No | Debt suspended[3] |

| | | | | | |
|---|---|---|---|---|---|
| | | | - | | |
| 990039183<br>500236112<br>054/01/2005 | Kiryat Arba Local Council | Property owners | **Kiryat Arba**<br>**9015001**<br>-<br>- | No | Approved |
| 990042125<br>511786717<br>- | Shilo- Publishers, Direct Mail, and Marketing Ltd[5] | Shilo- Publishers, Direct Mail, and Marketing Ltd | **Beit El**<br>**9063100**<br>-<br>- | No | "Burning"[6] |
| 991008967<br>580294080<br>- | Business Incubator - Samaria Economic Development Unit | Business Incubator - Samaria Economic Development Unit | **Ariel**<br>**4070005**<br>-<br>- | No | Debt suspended[3] |

Notes:

1. All the registrants entered "No" in the column asking if the database was used for direct mail. This column is therefore omitted from the chart here (but see note 5).
2. Further address details beyond area code (street, house number and mailbox details), which are listed in the register, have here been omitted.
3. The entries in the column on "Database status" saying "Debt suspended" presumably mean the registration fee has not been paid.
4. The entry on T.G. Biotechnological Institutes Ltd is the only one in this selection that says "Israel" in the column for "Country", although its place of establishment, Ma'ale Adumim (Area code 9842108) is indisputably in the Occupied West Bank. All the others leave this column (and the one asking for "State") blank.
5. Rather oddly, the entry for Shilo- Publishers, Direct Mail, and Marketing Ltd still says "No" in the column on the use of the database for direct mail.
6. The entry "Burning" in the column on "Database status" presumably means the matter (the payment of the fee?) is urgent.

### 5.1.3 Territoriality and transfers of personal data "abroad"

As is made clear in the 2011 Adequacy Decision on Israel itself, that decision only applies to Israel within its internationally-recognised 1967 borders. Indeed, as explained in section 3.2.2, at iii, above, this is a general EU approach: all adequacy decisions are inherently limited in their territorial scope to the third country or territory in question, and all transfers from a third country or territory with an adequacy decision to another third country without it constitute "onward transfers" for which special safeguards must be adopted.

It follows from what was established in the previous section that transfers of personal data by entities based in Israel within its 1967 borders, East Jerusalem or the Golan Heights, to other entities also based in any of these places, are not regarded as data exports ("data transfers abroad") under the Israeli PPA. As noted above, it appears that the same goes for entities in West Bank settlements.

By contrast, as also noted, it would appear clear that the PPA does not apply to processing of personal data by Palestinian individuals, companies or public bodies in the West Bank outside the Israeli settlements, and that any transfer of personal data from Israel proper to such individuals, companies or public bodies *are* regarded as transfers "abroad" in terms of the PPA.

In October 2020, Israeli lawyers have on our behalf asked the PP Authority for clarification of these issues, but by February 2021 no reply had been received.

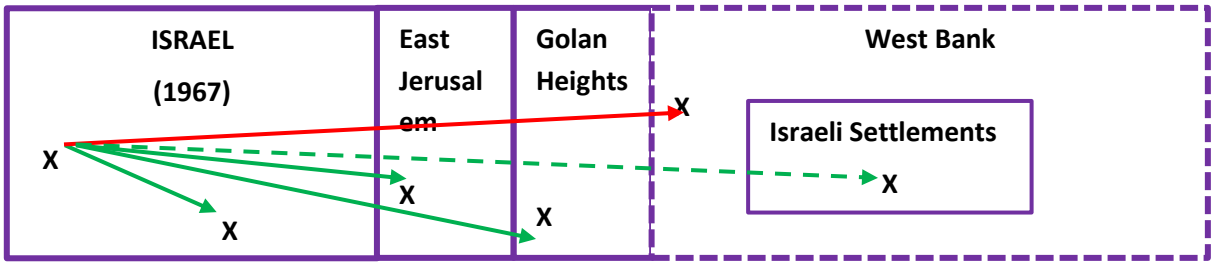
The above has a major impact on the question of transfers of personal data from the EU/EEA (including from EU institutions) to recipients in the different territories. The different legal views of the situation are illustrated in the two charts below.

**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**

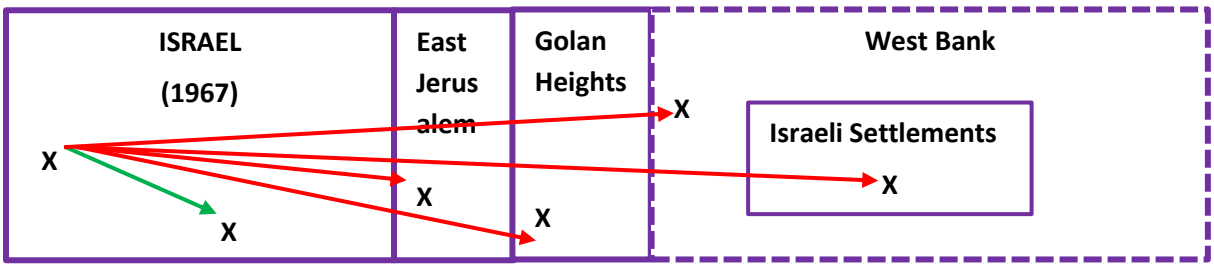



---

## II. EUROPEAN VIEW:

→ = internal domestic disclosure

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




For companies in Israel, East Jerusalem, the Golan Heights and in the Israeli settlements in the West Bank, the distinction in Israeli legal terms between internal domestic disclosures and transfers "abroad" (the green and red arrows in Chart 3.I) has no great repercussions because, as we have seen in section 3.2.3, above, the Israeli data export requirements are very lax: under the Privacy Protection (Transfer of Databases Abroad) Regulations adopted by the Government of Israel on 17 June 2001 under section 36(2) of the PPA,[185] it suffices that the recipient in the West Bank (or any other place outside of Israel proper) undertakes to comply with the requirements of the PPA also after transfer to those territories.

The regulations say nothing about the form or detail of these undertakings. They do not require the undertaking to be made to the Privacy Protection Authority, or indeed that the Authority has to be informed of such undertakings or provided with copies. There is no prescribed or recommended format for the undertakings relating to transfers from Israel to recipients outside Israel. More specifically, there is nothing comparable to the standard contract clauses (SCCs) for transfers of personal data from the EU/EEA to third countries that have not been held to provide adequate protection to such data, adopted by the EU Commission and recently updated (as discussed in section 2.2.4, above). It would appear that under the PPA, the undertakings can take the form of a broad general statement by the importer of the data to the exporter of the data that the recipient will abide by the rules in the PPA, without further specification of those rules or of how they should be applied by the recipient.

But it would appear that not even this is required for transfers of personal data from Israel proper to East Jerusalem or the Golan Heights or individuals, companies or public bodies in the Israeli settlements in the West Bank – because such transfers are in practice treated as internal domestic disclosures of the data rather than as transfers "abroad".

On the other hand, for the EU the distinction between transfers within Israel within its 1967 borders and the other transfers (all the red arrows in Chart 3.II) is fundamental. To recall again the stipulation in Recital (14) to the 2011 EU Commission Adequacy Decision on Israel:

> The adequacy findings pertaining to this Decision refer to the State of Israel, as defined in accordance with international law. **Further onward transfers to a recipient outside the**

185 See footnote 75, above.

> **State of Israel, as defined in accordance with international law, should be considered as transfers of personal data to a third country.** (emphasis added)[186]

Moreover, as noted in section 3.2.3, above, the EDPB has stressed in its "Adequacy Referential" that any initial recipient in Israel proper of personal data transferred from the EU/EEA "*shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision [on the final destination territory]*", and that "*[s]uch onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.*"

The recent EDPB recommendation on the need for "supplementary measures" (noted in section 3.2.2, above) makes clear that EU/EEA data exporters and their partner-data importers in third countries now have serious, onerous duties in that regard. They must use standard contract clauses in relation to the onward transfer, but in addition: must assess the law in the country or territory to which the data are to be onwardly transferred and check that the authorities there do not have undue access to the to-be-transferred data; if there is a risk of such access then they must consider adopting supplementary measures such as very strong encryption of strong pseudonymisation; if those measures might not prevent undue access, they must consult the data protection authority/ies in the relevant EU Member State(s); and they may not onwardly transfer the data if the data cannot be effectively protect against the undue access. But under the Israeli PPA, none of these steps of measures are required for transfers of personal data from Israel proper to East Jerusalem, the Golan Heights, or the Israeli settlements in the West Bank. In fact, even in respect of onward transfers of personal data from Israel proper to Palestinian recipients in the West Bank – which we believe *are* regarded as transfers "abroad" under the PPA – the requirements of the PPA are far less demanding than those required for those transfers by the GDPR if they involve EU data.

**It follows that 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 adequacy decisions and onward transfers in general, and with the stipulations in that regard in the 2011 Adequacy Decision on Israel in particular.**

**That is another major reason why the 2011 decision cannot be sustained under the GDPR.**

---

[186] Direct transfers of personal data from the EU to any of the OTs (including East Jerusalem and the Golan Heights, any Israeli settlements in the West Bank, or for that matter any other entities in the West Bank) are, from the point of view of EU law transfers to a territory that is <u>not</u> held to provide "adequate"/"essentially equivalent" protection to personal data, i.e., they may only take place if "appropriate safeguards" are provided, such as the use of SCCs. But there are two caveats to this. First of all, as explained in section 3.2.2, above, in view of the extensive – indeed, ubiquitous – surveillance in the OTs, especially the West Bank, "supplementary measures" such as strong encryption will be required for such direct transfers, in addition to the usual clauses in the SCCs (and these may well be insufficient given the technological expertise of the Israeli agencies). Secondly, as noted in section 4.2.4.iii, above, most if not all of EU communications with entities in the OTs is routed through Israeli communication- and Internet service providers (CSPs and ISPs) – and therefore involves, first transfers of the data to Israel proper, and then "onward transfers" of those data to the end-recipients in the OTs. The implications of this are discussed in Part 6.

## 5.2 Territoriality and differentiation

The above conclusion has implications also in relation to the EU "differentiation policy" and the relevant CJEU judgments. As explained in section 2.2, the aim of the policy, backed by the CJEU, is in particular to prevent the extension to the OTs (and individuals and companies in the OTs) of benefits and preferential treatments accorded to the State of Israel proper (and to individuals and companies in Israel proper). In that section, I provided examples in relation to preferential treatment in trade, EU research funding, recognition of Israeli product certification, etc. The territoriality clause in the 2011 Adequacy Decision is an early expression of that policy, in a legally binding EU instrument.

More specifically, the granting of a positive data protection adequacy decision to Israel can be seen as a similar benefit or preferential treatment: it means that transfers of personal data from the EU to Israel are in principle free.[187] However, under the differentiation policy, and under the adequacy decision, this benefit, this preferential treatment cannot be and is not extended to the OTs.

**The problem is that Israel's policy on the territorial application of its laws, and specifically the way in which the PPA is currently applied to East Jerusalem, the Golan Heights and (in practice) the Israeli settlements in the West Bank, clashes with the EU differentiation policy in relation to the processing of personal data (and with the 2011 Adequacy Decision, as noted in the previous section). The current Israeli policy is the data protection equivalent of labelling goods from the settlements "Made in Israel" or of allowing settlement entities to benefit from EU funding programmes.**

**Unlike in other areas of EU-Israel relations (incl. trade, EU funding, product certification, consumer labelling), the territorial limitations in the EU Adequacy Decision have not been enforced in practice. It appears that the EU quietly tolerates Israel's non-compliance with these provisions.**

## 5.3 Conclusion

**IN SUM: quite apart from the inadequacy of the Israeli PPA compared to the GDPR, and quite apart from the issue of undue access by Israeli state authorities to personal data transferred from the EU, the current Israeli policy on territorial application of the PPA is also fundamentally incompatible with the territorial clause in the 2011 Adequacy Decision and the wider EU differentiation policy towards Israel.**

**This is another reason why the current 2011 Adequacy Decision on Israel cannot be retained, or a new one issued, without a fundamental re-appraisal of the legal and practical situation.**

In the next part, after a brief summary of my conclusions, I discuss the implications.

[187] Although as noted in the previous section, the EDPB has recently held that this does not exempt data exporters from their duty to protect the transferred data from undue access by the Israeli authorities.

# 6. FINDINGS, IMPLICATIONS & CONCLUSIONS

## 6.1 Findings

In the previous parts, I have shown that the 2011 Adequacy Decision on Israel was fundamentally flawed and based on hopes of what the Israeli Privacy Protection Act (PPA) might look like after revision rather than on what it actually said; and that the PPA (which has been left largely unchanged since then) is manifestly not "adequate" in terms of the GDPR that imposes stricter requirements for adequacy, in relation to all three areas that must be assessed under the EDPB's "Adequacy Referential":

- the PPA provides far from "essentially equivalent" substantive protection to personal data compared to the GDPR;
- the Israeli Privacy Protection Authority is not clearly independent in GDPR terms; and
- the Israeli security agencies have excessive, undue access to personal data[188] including to personal data that have been transferred from the EU/EEA, both in the Occupied Territories (OTs) and in Israel proper.

Moreover, Israel currently applies its Privacy Protection Act (PPA) *de iure* (in terms of its domestic law) without distinction to East Jerusalem and the Golan Heights, and in practice also to the Israeli settlements in the West Bank. This is fundamentally incompatible with the stipulation on territoriality in the 2011 Adequacy Decision on Israel and the wider EU "differentiation policy" towards Israel and the OTs backed by relevant CJEU judgments.

In the next section, I discuss the implications of these findings for future (and indeed current) transfers of personal data from the EU/EEA to Israel proper and the OTs, in the light of both the GDPR requirements on data transfers and of this "differentiation policy".

## 6.2 Implications in three scenarios

In relation to transfers of personal data and the question of the adequacy of the Israeli PPA, the implications of my findings vary depending on whether the EU Commission will, after the current review of its 2011 Adequacy Decision on Israel, issue another positive decision, or not. There are in fact three scenarios in this respect:

A. The EU Commission does nothing; the 2011 decision is allowed to continue to apply;

B. The EU Commission issues a new positive adequacy decision on Israel;

C. The Commission repeals or suspends the 2011 decision without replacing it (for now).

---

[188] In this part of my opinion, too, the phrase "**undue access**" (by third country agencies, to personal data transferred to the third country from the EU) is used as shorthand for access by such agencies under laws or practices of the third country or territory concerned that do not meet the standards set out in the European Data Protection Board's "European Essential Guarantees" on such access (that reflect the CJEY case-law on the issue).

My findings argue in favour of the third scenario (C). However, as noted below under that heading, the consequences for Israel – or indeed any third country – of not having a positive adequacy decision are significant.[189]

This is all the more so because the absence of an adequacy decision under the GDPR also affects flows of personal data from any EU institution or body to the third country concerned, such as in relation to EU programmes. This is the case because the regulation that applies to processing of personal data by those institutions, Regulation 2018/1725,[190] cross-refers to the decisions under the GDPR in that respect.[191] The European Data Protection Supervisor has in fact issued orders to the EU Institutions to map their data transfers to the USA and carry out Transfer Impact Assessments of all such transfers in the light of the *Schrems II* judgment.[192]

It would be surprising if a similar policy were not to be adopted in relation to other third countries with extensive surveillance programmes that allow for undue access to personal data transferred from the EU, by agencies of the third countries concerned. As explained elsewhere, this would appear to be a clear implication in relation to the other "5EYES" countries that cooperate closely with the USA in such programmes: the UK, Australia, Canada and New Zealand[193] - but the same is likely to apply to other third countries that allow for undue access, be they Israel or the People's Republic of China.

The Commission – and the Member States through their involvement in the process, in particular in the Article 93 Committee[194] – may decide, for political reasons, to maintain the status quo in which Israel is deemed to provide adequate protection (Scenario A). This is likely to be challenged in view of the much stricter criteria for adequacy ("essential equivalence") and the serious inadequacies in the Israeli PPA and of the information about indiscriminate surveillance in Israel and the OTs – but it would buy the Commission (and Israel) time.

---

189 Cf. the implications for the UK and the other "British Islands" (Guernsey, Jersey and the Isle of Man), of a possible refusal by the EU Commission to issue a positive adequacy decision on the UK for after the post-Brexit transition period, discussed in the Executive Summary of the two parts submission to the EU by Douwe Korff and Ian Brown on the inadequacy of UK data protection law in general and in view of UK surveillance laws, (footnotes 26 and 115, above).

190 Full title:Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

191 See Articles 47 and 48 of Regulation (EU) 2018/1725.

192 EDPS, Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling, 29 October 2020, available at:
https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf

193 See section 4.3 in the Executive Summary of the two parts submission to the EU by Douwe Korff and Ian Brown on the inadequacy of UK data protection law in general and in view of UK surveillance laws, (footnotes 26 and 115, above).

194 On the role of this committee in the process, see section 2.2 in Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general, Part One (footnote 26, above).

For the same reasons, the second scenario (Scenario B – a new positive adequacy decision) is perhaps the least likely. The EDPB – which is a stronger and more self-confident body that its predecessor, the Article 29 Working Party – must give its opinion on the issue[195] and in my view, if it takes the matters set out in this paper into account, is unlikely to issue a positive opinion, and the Commission could really not ignore a negative one. The European Parliament, too, would likely take a dim view of an unwarranted new positive adequacy decision. And as Maximillian Schrems has shown, even determined individuals can successfully challenge wrongly issued adequacy decisions, and the GDPR also allows for "representative actions" to be brought by certain not-for-profit organisations.[196] But below, all scenarios will still be considered.

### A. The EU Commission does nothing; the 2011 decision is allowed to continue to apply

As explained below, if the 2011 decision is allowed to continue to apply, then that decision will stand for the time being – but it can be challenged (albeit in a cumbersome process). Moreover, under the GDPR, as very recently clarified, this does not absolve the data exporter from liability if the data are unduly accessed by state agencies in the third country. And the European data protection authorities can also challenge transfers in individual cases.

Moreover (as also discussed below), the situation in relation to the territorial application of the decision and in relation to the issue of "onward transfers" would be complicated – or indeed, as I will conclude, untenable.

***The decision stands …***

In this scenario, transfers of personal data to Israel proper (within its 1967 borders) can in principle continue: as the Court of Justice made clear in its *Schrems II* judgment, until such time as a Commission adequacy decision is declared invalid by the Court of Justice (or, one may add, withdrawn or suspended by the Commission itself), the decision stands and is binding on the Member States and their data protection authorities (now more commonly referred to as supervisory authorities).[197]

***… but can be challenged (albeit only in a cumbersome process) …***

Individual data subjects can challenge transfers made under an adequacy decision on the basis that the adequacy decision is invalid – but the process is cumbersome:[198]

> even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the

---

195 *Idem*.

196 See Article 80 GDPR. On 30 September 2020, Max Schrems's NGO, *noyb*, was granted status to bring such actions in Belgium, see the Official Journal of 8 November 2020, available at: http://www.ejustice.just.fgov.be/cgi/article_body.pl?numac=2020015708&caller=list&article_lang=F&row_id=1&numero=1&pub_date=2020-10-08&language=fr&du

197 *Schrems II* judgment, para. 118.

198 *Idem*, para. 120.

> transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling [to the CJEU] for the purpose of examining its validity.

***… does not absolve the data exporter from liability …***

Until recently, EU-based data exporters generally believed that a positive adequacy decision on a third country effectively gave them a "free pass" to transfer personal data to recipients in that country. However, the EDPB, in its very recent recommendation on supplementary measures that may be needed in relation to transfers to countries without an adequacy decision, made clear that such measures may also be required in relation to transfers to countries with an adequacy decision (and indeed even for transfers within the EU/EEA):[199]

In other words, if there is a risk that the authorities in a third country, *including a third country with an adequacy decision*, will unduly access[200] personal data that are transferred to that country, then the EU-based data exporter will have to take "appropriate" measures to protect the data against this undue access. Failure to effectively ensure such protection will constitute a failure to prevent "unauthorised access" in terms of Article 4(12) – and that exposes the data exporter to significant administrative fines and costly suits for compensation for damages (which includes immaterial damages).

***… and EU data protection authorities can still intervene in relation to specific cases:***

In addition to the above, under Article 3(1)(b) of the 2011 decision the supervisory authorities of the EU Member States also have the right, *ex proprio moto* or in response to complaints, to "exercise their existing **powers to suspend data flows to a recipient in the State of Israel** in order to protect individuals with regard to the processing of their personal data" *inter alia* when:

> there is *a substantial likelihood that the standards of protection are being infringed*, there are reasonable grounds for believing that *the competent Israeli authority is not taking or will not take adequate and timely steps to settle the case at issue*, the continuing transfer would create *an imminent risk of grave harm to data subjects* and the competent authorities in the Member State have made *reasonable efforts* in the circumstances to provide the party responsible for processing established in the State of Israel with *notice* and an opportunity to *respond*.
>
> (*Italics* added)

As the references to "*data flows to **a** recipient in the State of Israel*" and "*settl[ing] the case*" suggest, this possibility is intended for specific individual cases. The clause moreover assumes that the relevant EU Member State supervisory authority first seeks to address the issue in exchanges with "the party responsible for processing established in the State of Israel" and/or

---

199 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (footnote 48, above), para. 78.

200 See footnotes 35 and 187, above.

through the good offices of its Israeli counterpart, i.e., the Privacy Protection Authority. And this power to suspend data flows is subject to important conditions, as indicated by the italics in the quote above.

Nevertheless, in my opinion, such a suspension of data flows to an Israeli recipient is an avenue that may well be resorted to in relation to some special cases – in particular, in relation to surveillance by the Israeli security agencies (more specifically, Unit 8200) of communications between, on the one side, EU officials, or journalists, politicians or other individuals and on the other side entities or individuals in Israel or the OTs. Europeans interested or active in the Boycott, Divest and Sanctions (BDS) movement or individuals (and even officials) involved in the investigation of alleged war crimes by Israel, may be particularly targeted by Israeli surveillance, as covered in section 4.2.4, above.

**The general implications of this scenario are that the 2011 Adequacy Decision on Israel would formally continue to apply but would be at risk of fundamental challenges that are ultimately likely to succeed. In other words, although this would buy some time for the European Commission (and Israel), it is not a sustainable solution in the long or even medium term.**

**In addition, a decision by the Commission to not rescind the 2011 Adequacy Decision on Israel would be in flagrant breach of the (since then much more emphatically declared and applied) EU "differentiation policy" towards Israel and the OTs, given Israel's non-compliance with the territorial clause in the Adequacy Decision.**

**These issues could not simply be ignored for political expedience reasons, given that under the GDPR the European Commission was and is under a legal duty to review the adequacy decisions granted under the 1995 Data Protection Directive by May 2020 (Article 97(2)(a) read together with Article 45(3) and (5) GDPR) – i.e., the Commission is already overdue to produce the results of these reviews.**

**The Commission could and should have started discussions on Israeli data protection reforms already years ago, when it became clear that no significant changes were being made to the PPA (in spite of the prospects of such changes being a major reason for the 2011 adequacy decision). The Commission could and should certainly have commenced such discussions urgently in 2016, after the coming into force of the much more demanding GDPR.**

**Crucially, as noted in relation to scenario B, below, such discussions (as and when they finally take place) will be demanding and take some considerable time. Given that this matter is already unduly delayed, the 2011 decision would have to be suspended pending those discussions. In reality, therefore, this scenario (like scenario B) effectively morphs into Scenario C.**

**In my opinion, it follows that the 2011 Adequacy Decision is untenable, even in the short term.**

## B. The EU Commission issues a new positive adequacy decision on Israel

Because of the glaring deficiencies in the PPA compared to the GDPR, and because of the indiscriminate surveillance that is allowed under the law in both the OTs and to a considerable extent also in Israel proper, it is extremely unlikely that the EU Commission will be able to issue another positive adequacy decision on Israel under the GDPR (or indeed that the EDPB would issue a positive opinion) if those matters remain unchanged. And any such decision would be wide open to legal challenge. But it may still be noted that my earlier findings would still have implications for such a new decision.

First of all, any such new decision would have to reflect more clearly the EU "differentiation" policy towards Israel. It would have to "unequivocally and explicitly indicate [its] inapplicability to the territories occupied by Israel in 1967", namely the West Bank including East Jerusalem, the Gaza Strip and the Golan Heights; and it would have to equally "unequivocally and explicitly" state that any passing on of personal data sent from the EU to Israel proper to any of the OTs constitute "onward transfers" in terms of EU law (in particular, the GDPR and Regulation 2018/1725).

This would create the very same conflict we noted in the previous scenario, in that under the PPA as it stands, Israel does not impose the restrictions required by EU law on what in EU law clearly constitutes "onward transfers" of the data to East Jerusalem or the Golan Heights, and to the Israeli settlements in the West Bank. In other words, the EU could really only adopt a new positive adequacy decision on Israel if Israel agreed to change its practice in this regard.

Moreover, given the – from the EU perspective, manifestly undue – access by the Israeli intelligence agencies to personal data that may be transferred from the EU to Israel or to any of the OTs, such a new adequacy decision would not exempt EU data exporters from their (recently clarified) duty to adopt appropriate measures to protect the data they transfer from such undue access even in respect of third countries with adequacy decisions, or from liabilities in respect of such transfers. Again, this could only be avoided if Israel were to agree to change its law and practices, here: in relation to its currently excessive surveillance.

Such changes could not be achieved by the EU alone: really the only way to address the issues would be to work with Israel on new data protection rules, "essentially equivalent" to the ones in the GDPR, and on much stricter limitations on access to personal data transferred from the EU to Israel or the OTs including effective remedies against undue access. Likewise, the EU would have to work with Israel to change its rules and practice in respect of onward transfers of EU/EEA personal data to the OTs (which should not be treated as internal-domestic disclosures).

In order to again being held to provide adequate – and this time, "essentially equivalent" – protection to EU law, the outcome of the EU – Israel discussions would have to be that Israel would:

- bring the substance of its Privacy Protection Act into line with the GDPR;
- make the Privacy Protection Authority truly independent and provide it with appropriate powers and resources;
- change its law and practices in relation to surveillance (In Israel proper and in the OTs) so that they meet the "European Essential Guarantees" relating to surveillance; and

- ensure that flows of personal data from the EU/EEA via Israel proper to any of the Occupied Territories (including East Jerusalem and the Golan Heights as well as the Israeli settlements in the West Bank) will be treated as "transfers of personal data abroad".

In some of these respects, consideration could perhaps be given to the adoption of special Israeli rules on the processing of personal data transferred to Israel from the EU/EEA – just as the EU – US Privacy Shield made special arrangements for EU – US transferred data without the USA adopting a broad privacy/data protection law at the federal level. However, this would be a very complicated undertaking and – as the *Schrems II* judgment has made clear – it could not rely on "self-certification" by Israeli entities and contract clauses, because those cannot override the legal rules giving the authorities undue access to the transferred data

In my opinion, as a first necessary (but not sufficient) step towards adequate data protection, Israel would have to amend its PPA (or replace it with a new law) so as to *at the very least* meet the requirements of Council of Europe Convention 108+ and sign and ratify that convention.

Beyond that, the aim should be for Israel to (a) amend the PPA (or replace it) so as to really make its data protection legislation generally "essentially equivalent" to the EU rules (the GDPR in particular); and (b) limit access to personal data by the Israeli intelligence agencies in line with the European Essential Guarantees on surveillance.

In relation to territorial differentiation between Israel and the OTs, the EU would have to obtain Israel's agreement to treat onward transfers of EU/EEA personal data to the OTs as "transfers of personal data abroad". Israel would have to adopt a measure to that effect, obliging Israeli data controllers and processors to treat onward transfers of EU/EEA data to the OTs in this way, with the appropriate safeguards for onward transfers to a non-adequate territory.

Whether this is feasible is a separate matter. On the one hand, it is perhaps more conceivable that EU territorial requirements could be met through a specific Israeli measure related to transfers of EU/EEA data only, without amending the PPA itself. Such a solution would be broadly similar to past instances in which Israel agreed, after discussions with the EU, to abide by the EU's differentiation between its territory under international law and the OTs: the technical arrangement on trade (2004), the funding guidelines for Horizon 2020 and other EU programmes (2013), and certification of organic and animal-based products (2014 onward), as described in section 2.2 above.

On the other hand, the example of attempts to address deficiencies in the US legal regime in relation to data transferred from the EU/EEA without changing US law overall is not encouraging: both the initial EU–US Safe Harbour agreement and its successor, the Privacy Shield, were held to be invalid by the EU Court of Justice because the Commission did not take sufficient account of US mass surveillance.

In practice, one way or the other, this would take some considerable time (with limited prospect of success), and given that (as explained earlier, at A) this matter is already unduly delayed, the 2011 decision would have to be suspended pending the discussions. In reality, therefore, this scenario (like Scenario A) effectively morphs into Scenario C.

## C. The Commission repeals or suspends the 2011 decision without replacing it (for now)

It follows from my analyses of scenarios A and B that the only realistic option in legal terms is for the Commission to withdraw or suspend the 2011 Adequacy Decision on Israel and, at least for the time being, to not issue a new positive adequacy decision on Israel; and to commence discussion with Israel on how the serious issues and conflicts between EU and Israeli data protection law can be resolved: see my summary, above, at B, of the changes or steps that would be required of Israel in order for it to again be held to provide adequate – and this time, "essentially equivalent" – protection to EU law.

The obvious implication would be that after such a withdrawal or suspension and during such discussions Israel would have to be treated like any other third country that had not been granted a positive adequacy decision. This would mean that regular transfers of personal data that are processed subject to the EU GDPR (or, for the EU Institutions, Regulation 2018/1725) to Israel proper would be permitted only if "appropriate safeguards" were put in place between the EU-based data exporter and the Israel-based data importer.

If the 2011 decision is repealed or suspended, and such discussions on reform are undertaken, there would, during that time, not be an adequacy decision on Israel in place. Israel would therefore, for that period, for EU data protection/data transfer purposes, be in the same category as the Occupied Territories already are: regular direct transfers of personal data from the EU/EEA to those territories (or any entity in those territories) – and onward transfers of personal data from the EU/EEA to those territories, via Israel – may all already only take place if such "appropriate safeguards" are in place (although at the moment this is not effectively enforced).

As explained in section 3.2.3, above, those safeguards include, for regular data transfers within a group of enterprises, approved Binding Corporate Rules (BCRs); for other companies, standard contract clauses (SCCs); for the EU institutions, data transfer agreements specifically approved by the European Data Protection Supervisor; and for public bodies in the EU in relation to processing subject to the GDPR, "administrative arrangements" that have been authorised by the relevant data protection authority (see Article 46 GDPR).

However, as also explained there, these do not suffice in relation to third countries that engage in undue surveillance (surveillance that does not meet the European Essential Guarantees for surveillance issued recently by the European Data Protection Board). Rather, as the Court of Justice of the EU has made clear in its *Schrems II* judgment, in relation to such third countries, "supplementary measures" must be adopted to ensure that the transferred data will be protected against the undue surveillance. The EDPB has also recently issued initial guidance on what this may entail. If there are no "supplementary measures" that can effectively protect against undue surveillance in the third country concerned, the data may not be transferred.[201]

[201] See footnote 48, above.

All this would, for that period during which no adequacy on Israel is in place, apply to all the above-mentioned transfers alike: to direct transfers from the EU/EEA to Israel proper; to (presumably relatively rare) direct transfers from the EU/EEA to (any recipient anywhere in) the OTs; and to the more usual indirect (onwards) transfers from the EU/EEA to recipients in the OTs routed via Israel proper.[202]

Suffice it to note here that given the sweeping surveillance carried out by the Israeli intelligence agencies, these EU requirements will create very significant obstacles to transfers of personal data from the EU to Israel and the OTs.

## 6.3 Conclusions

All the adequacy decisions adopted by the European Commission under the 1995 Data Protection Directive must be reviewed (in fact, already should have been reviewed) in the light of the stricter conditions on such decisions imposed by the GDPR and the case-law of the CJEU. This includes the 2011 Adequacy Decision on Israel. Renewal should not be taken for granted.[203]

I believe that I have shown in this opinion that the 2011 Adequacy Decision on Israel was fundamentally flawed and based on hopes of what the Israeli Privacy Protection Act (PPA) might look like after revision rather than on what it actually said; that the PPA (which has been left largely unchanged since then) is manifestly not "adequate" in terms of the GDPR; and that the application by Israel of its Privacy Protection Act (PPA) to East Jerusalem and the Golan Heights, and in practice also to the Israeli settlements in the West Bank, is fundamentally incompatible with the stipulation on territoriality in the 2011 Adequacy Decision on Israel and with the wider EU "differentiation policy" towards Israel and the OTs.

Moreover, I believe that I have shown in this last part of my opinion that allowing the 2011 EU Commission adequacy decision on Israel to continue to apply (Scenario A in section 6.2, above) is not only not a sustainable solution in the long or even medium term, because that situation is open to immediate challenges that are likely to succeed (albeit after some delay), but in fact also untenable in the short term because of the EU's failure to ensure Israel's compliance with the territorial clause in the Adequacy Decision. At the very least, in this scenario, the Commission would have to enter into discussions with Israel about amending its data protection regime – and those discussions would be intricate and lengthy. Given that this matter is already unduly delayed, the 2011 decision would have to be suspended pending those discussions. In reality, therefore, this scenario (like scenario B) effectively morphs into Scenario C (see below).

---

[202] Direct transfers of personal data from the EU/EEA to Israel are relatively rare because almost all communications between the EU/EEA and Israel are routed through Israel-based communication- and Internet service providers: see section 4.2.2.iii, above.

[203] See, for instance, the discussion on Guernsey, Jersey, the Isle of Man, Canada and New Zealand in sections 4.2 and 4.3 in the Executive Summary of Douwe Korff and Ian Brown's submission to the EU on The inadequacy of UK data protection law (footnote 115, above). There, it is argued that the pre-Snowden adequacy decisions on these territories cannot be renewed, in particular, in the light of the surveillance activities they are involved in (in the case of the Channel Islands, their link with the UK's activities).

I believe that the Commission could also not, at this time, issue a new positive adequacy decision on Israel (Scenario B) because the current deficiencies in Israeli law are so manifest that the Commission would, in this scenario, too, at least have to try and negotiate changes to the PPA to bring it in line with the EU requirements.

In other words, it follows from my analyses that the only option that is compatible with the standards set by the Court of Justice of the EU in recent judgments in both the areas of data protection and in relation to territorial differentiation, is for the Commission to withdraw or suspend the 2011 Adequacy Decision on Israel and to try and persuade Israel to bring its data protection law and practice in line with EU standards and territorial requirements, and to end indiscriminate mass surveillance.[204] This is described in Scenario C in section 6.2, above.

Until such changes are made, there would be very significant obstacles to transfers of personal data from the EU to Israel and the OTs. But the overall implication is clear:

Israel will have to choose: It can be granted a positive EU adequacy decision and then enjoy free personal data exchanges with the EU if it adopts data protection standards and rules that are "essentially equivalent" to the EU ones, amends it surveillance laws and practices to meet the European Essential Guarantees on surveillance, and starts treating onward transfers to the OTs as transfers abroad, at least as concerns EU data.

Or it will forego such a decision and will then have to face and accept the negative consequences in the form of restrictions on the free flow of personal data from the EU/EEA to Israel.

- o – o – o -

Douwe Korff (Prof.)
Cambridge (UK), 4 February 2021

[204] In fact, an opportunity for review has just presented itself: on 29 November 2020, the Israeli Ministry of Justice published an open call for submissions for amendments to the 1981 Privacy Protection Act, see:
https://www.mondaq.com/privacy-protection/1013030/call-for-submissions-amendments-to-the-privacy-protection-law?email_access=on
https://www.gov.il/he/departments/publications/Call_for_bids/amendment_privacy_protection
(original call in Hebrew).
However, the EU should not repeat its mistake from 2011, when it issued its first positive adequacy decision on Israel, largely on the basis of expectations that the PPA would be updated and improved – but which never happened.