India’s 2023 data privacy Act: Business/government friendly, consumer hostile

The government can collect much personal data without consent and restrict transfer of personal data to any overseas country. Graham Greenleaf analyses the impact of the new law. Suddenly, it was completed. Within a week of introduction into Parliament, India’s Digital Personal Data Protection Act, 2023 was passed by both houses with no debate, and no requirement of committee consideration. It received Presidential assent on 11 August.

The EU-US Data Privacy Framework: A durable solution or heading for Schrems III?

The deal eliminates the burdensome requirements of conducting transfer impact assessments. Ceyhun Necati Pehlivan of Linklaters analyses this and other practical implications.

In today’s digital era, data flows are essential to organisations of all sizes and in all sectors of the economy. They underpin the global economy and international trade in goods and services.

Free place at a PL&B event

Report subscribers can obtain a free place at a PL&B organised in-person or online event when booked at least seven days in advance. This arrangement excludes the International Conference held annually in July. More than one free place available with Multiple and Enterprise subscriptions

www.privacylaws.com/events

PL&B Services: Conferences • Roundtables • Content Writing
Recruitment • Consulting • Training • Compliance Audits • Research • Reports
Data transfer scene evolves but a global solution is needed

In this issue, we report on some practical points for organisations to consider regarding the EU-US Data Privacy Framework (p.1). Late September, the UK finally announced that from 12 October 2023, UK organisations can transfer personal data to US organisations certified to the “UK Extension to the EU-US Data Privacy Framework” (p.12).

However, in the long term, a global solution is needed. The G7 DPAs have been discussing data flows in their meetings and promote “Data Free Flow with Trust” (p.22). The G7 digital ministers also work on AI and are expected to meet at some time before the end of the year to issue a paper on generative AI. The aim is to develop international guiding principles alongside a code of conduct.

DPAs are looking into how AI can help them in their work (p.20). We at PL&B are currently planning a one-day workshop to identify benefits for the busy DPO in terms of managing the role with the help of AI. Please register your interest at info@privacylaws.com for this one-day seminar on 23 January 2024, to be hosted by the Macquarie Group in London.

As we were preparing to go to print, the US State of Delaware enacted a privacy law. This is now a trend in the US – but there is still no progress on a privacy law at the federal level. India, on the other hand, suddenly ended its long legislative process by adopting a law. Read a detailed analysis of this Act on p.1 by Professor Graham Greenleaf, PL&B Report’s Asia-Pacific Editor.

A category of its own are countries that a long time ago gained an adequacy status according to the European Union 1995 Data Protection Directive, and now need to modernise their laws to meet the higher EU GDPR standard. Israel is one of them (p.16). What is puzzling is why it takes the EU Commission such a long time to issue its evaluation of the countries that have an old adequacy decision.

Other developments include Saudi Arabia’s 2021 privacy law, now in force since 14 September (p.13).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.
2023. The Act, or particular provisions, will come into force on dates notified in the Official Gazette. India’s Minister for Electronics and IT says the government may allow as little as six months for compliance, but not as long as two years, after consultation with industry. Other than the United States, India has until now been the most significant country, economically and politically, not to have a comprehensive data privacy law.

Five years after the committee chaired by former Justice BN Srikrishna delivered its report, recommending a strong international-standard Bill, this proposed law was progressively weakened by a succession of Government-redrafted Bills, and by recommendations of a joint Parliamentary committee report. The final Act inherits many of these accumulating weaknesses, but is closer to a completely new draft, rather than a redraft of any previous version. The lack of any consultation on this Bill is therefore a result of a more authoritarian political system.

This article focuses on the resulting Act, rather than its history, and aims to identify which are the main societal interests that the Act is likely to benefit the most, including the Indian business sector, foreign businesses, individuals (consumers and citizens), and the Indian government.

SCOPE AND SPECIAL CATEGORIES

The Act applies to all levels of government in India (Central, State and local), and to the private sector, all of which come within the meaning of “Data Fiduciaries” (s2(i)). In Indian legislation, the “State” encompasses all these levels of government, and this is crucial in this Act.

The Act only applies to the processing of “digital personal data” which means that it is collected in digital form (or subsequently digitised) (s3(a)), so paper-based transactions are exempt, except for such data as is digitised.

“Personal data” is given a conventional definition, meaning “any data about an individual who is identifiable by or in relation to such data” (s2(t)). Such individuals are “Data Principals” (data subjects), and those who control the use of personal data about them are Data Fiduciaries (controllers), assisted by contracted Data Processors.

There are no separate categories of data, such as “sensitive data”. Special protection of specified categories of data based on sensitivity is typical in post-1995 data protection laws. As a result, there is no requirement in India to take special care with data about such matters as race, caste or tribe, criminal records, religious or political beliefs, sexual orientation, health, financial affairs, biometrics, genetic characteristic or any other characteristics. The previous Indian draft Bill did protect “sensitive personal data” including the above matters, except race or criminal record. This Act is therefore an abrupt departure from both the previous draft and international standards.

There is however, in effect, a separate category of special protections for the personal data of children: verifiable consent of the child’s parent or lawful guardian must be obtained before any processing (and of persons with disabilities who have lawful guardians); processing likely to cause any detrimental on the well-being of a child must not occur; tracking, behavioural monitoring or targeted advertising must not occur in relation to children (s9(1)-3). However, the Government makes exceptions (s9(4)-(5)). On its face, this is strong protection for children’s privacy. But it is also bizarre and undesirable that all persons with any disabilities are equated with children.

Another important weakness in the meaning of “personal data” is that it does not include any data which the Data Principal has made publicly available, or anyone else has done so as a result of a legal obligation (s3(c)). Internationally, most countries take the EU GDPR approach that such information is still “personal data”, but a significant minority of countries (e.g. Australia, Singapore, Malaysia) take an approach similar to India. Because of the rise of social media services, this is now a far more dangerous provision.

EXEMPTIONS: NUMEROUS WEAKNESSES

The Central Government has very broad powers to utilise exemptions from the Act, both complete and partial:

• It may completely exempt processing by specified State instrumentalities, on very broad grounds of State interests (s17(2)(a)).
• It may notify as exempt certain Data Fiduciaries, or classes of Data Fiduciaries (s17(3)), either from the public or private sectors. It can also, within five years, declare that any provisions of the Act will not apply to Data Fiduciaries or classes of same, for a specified period (s17(5)). Either provision may result in broad exemptions, for reasons which are not controlled by any objective standard. They could also result in undesirable and potentially anti-competitive case-by-case exemptions.
• It may also completely exempt processing necessary for research, archiving or statistical purposes if the personal data is “not to be used to take any decision specific to an individual”, and is carried out in accordance with prescribed standards. (s17(2)(b)). It will be very important, and potentially dangerous, if such processing can be for commercial “research”, for example the creating of Large Language Models (LLMs) for generative AI.
• “Automatic” exemptions, not depending on Government notifications, are also very significant:
  • The State or its instrumentalities are automatically exempt (17(4)) from data erasure obligations, both automatic and on request (s8(7) and s12(3)), and from making corrections etc. on request, unless the data is being used to make decisions about a person (s12(2)).
  • There are also numerous automatic exemptions from parts of the Act for processing in relation to enforcing legal rights, judicial or regulatory functions, law enforcement, company reorganisations, and credit defaults (s17(1)). These are exemptions from most of the Act, but not from Data Principal’s rights, some Data Fiduciary obligations, or from the s16 export prohibition.

The combination of the first category s17(2)(a) of notified exemptions, and the first category of automatic exemptions (s17(4)) means that the Central Government (and to a lesser extent, other governments) can collect...
much personal data without consent, and can accumulate personal data without ever deleting it, or even ensuring its accuracy in most cases. It is a recipe for creating comprehensive government surveillance. This may be one of the most important deficiencies of the Act. It may also make the Act vulnerable to claims that it unconstitutional because of lack of proportionality, based on Puttaswamy’s setting out of the constitutional right of privacy (see later).

**DATA LOCALISATION**

Some concept like “critical data” is increasingly used to identify data which (in various places) can only be stored within the country (so no exports are allowed, and processing must occur within the country), or a copy of which must be kept within the country (and exports and overseas processing are then allowed). No such explicit “data localisation” provisions are included in this Act, but that is not the end of the matter. First, it is possible that data export restrictions (see below) could be used for this purpose.

Second, there are already separate laws of major importance in India which do require data localisation, including the Companies Act 2013 s94 and the Companies (Accounts) Rules 2014, which require covered organisations to store financial information at the registered office of the company; an April 2018 circular by the Reserve Bank of India (RBI), “Storage of Payment System Data”, which “ordered all payment companies to keep all information relating to payment systems” on servers in India; and the IRDAI (Maintenance of Insurance Records) Regulation, 2015, s3(9) which requires covered organisations to store insurance data within India.

**EXTRA-TERITORIALITY, EXPORT BLACKLIST AND OUTSOURCING EXEMPTION**

Processing of data outside India on Data Principals (data subjects) in India is within the extra-territorial jurisdiction of the Act, but only for transactions offering goods and services (s3(b)), and not for monitoring as in the EU.

The Government may by notification restrict transfer of personal data to any overseas country or territory (s16) – “blacklisting”. Until such notifications are made, data may be transferred anywhere. The Data Protection Protection Board (see below) has no role in determining which countries are blacklisted. There is no “positive” test (e.g. “adequacy” or equivalence to this law) to justify transfers, only a negative blacklist (once made) for which the Act does not state any objective criterion for inclusion. The export blacklist is therefore completely within the discretion of the Central Government, and all other countries are, by default, included on the data export “whitelist”. For example, there is no restriction at present, on data exports to the US, despite its lack of general data privacy laws. In fact, India’s position on data exports, until it creates a blacklist, is closest to that of the US.

The Act includes an “outsourcing exemption” from its operation, excluding from its scope any processing within India of personal data of persons outside India, pursuant to a contract (s1711(d)). So, outsourced processing in India of data on EU residents is not protected by the Act, which should be fatal to India obtaining a positive “adequacy” assessment from the EU (which it has failed to do twice before, the most recent being in 2013). EU companies wanting to outsource processing to India would have to rely on the use of GDPR Standard Contractual Clauses (SCCs, as revised, June 2021) for each outsourcing contract, which means the situation will be unchanged from what it is now. The “new” SCCs, revised by the European Commission in 2021 in light of the Schrems II decision of the CJEU (Case C-31/18) includes additional clauses such as Clause 14 which requires the Indian importer, and the EU exporting party to prepare a data transfer impact assessment (DTIA) which, among other things, assesses Indian laws requiring disclosure of data to public authorities, or authorising access by such authorities. The difficulties in applying SCCs in the Indian context are beyond the scope of this article, but they are not trivial.

Countries which have positive adequacy findings from the EU (e.g. the UK, Japan and Korea) will not be able to outsource to India without taking similar precautions, or they may risk their EU adequacy status. In contrast, outsourcing from the US could carry on without additional restriction.

**LEGITIMATE PROCESSING**

Processing by Data Fiduciaries must be either with consent of the Data Principal, or for specified legitimate uses (s4), and must not be for an unlawful purpose.

Consent by Data Principals, for specific purposes, has a strong definition: “The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose” (s6(1)). This is comparable to the definition of consent in the EU GDPR (art. 4(11)) and is stronger because the inclusion of “necessary for such specified purpose” adds a data minimisation requirement. Consent may be withdrawn at any time, with equivalent ease to consenting (s6(4)). Consents to waive rights under the Act, or obligations of Data Fiduciaries, or of any other law, are invalid (s6(2), s8). A Data Principal “may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager” (s6(7)), who must be registered with the Board (s6(9)). Consent must be obtained by the Data Principal being given a notice accompanying or preceding the request, specifying the proposed purpose of processing, how rights may be exercised, and how complaints may be made (s5(1)). These requirements are repeated in s6(3) which adds that the contact details of a Data Protection Officer (DPO) or equivalent person must be given. For data already collected prior to the Act’s commencement, the Data Fiduciary must, as soon as reasonably practicable, give the same notice (s5(2)). The Data Principal may request the notice in a common language in India (s5(3)).

The “legitimate uses” on the basis of which personal data may be processed without consent are very broad. They are (s7):
- It can be processed “for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary”
is made. Unless the Data Principal requests a copy of their record, these uses will usually remain secret uses. Nor are these “legitimate uses” required to have any close connection to the original purpose of use.

These “legitimate uses” are particularly dangerous for the uses by government instrumentalities under s7(b) and s7(c), which could result in very large dossiers. This is particularly so because the right to automatic erasure of data once its specified purpose is no longer being served is waived wherever retention is required by law (s12(3) – more details below). Some critics consider that the potential for data to be combined, with exemptions from erasure, creates the risk of “profiling of citizens”.12

OBLIGATIONS OF DATA FIDUCIARIES AND SIGNIFICANT DATA FIDUCIARIES

All Data Fiduciaries (data controllers), including those in government, have the following normal obligations:

• To “ensure its completeness, accuracy and consistency”, if it is “used to make a decision that affects the Data Principal or disclosed to another Data Fiduciary” (s8(3)).
• To “ensure effective observance of the provisions” of the Act and rules, by implementing “appropriate technical and organisational measures” (s8(4)). This could come close to the EU GDPR’s “demonstrable accountability”.
• To take “reasonable security safeguards to prevent personal data breach” (s8(5));
• To “give the [Data Protection] Board and each affected Data Fiduciary” notice of any data breaches, in a prescribed manner and form (s8(6)). The obligation to notify individuals of every breach is immediate, on the face of the section, but the manner and form to be prescribed may well cut this back somewhat.
• To “erase personal data, upon the request of the Data Protected or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier” (s8(7)). Data Processors are required to do likewise. Erasure is therefore supposed to be automatic, not dependant on a request. However, erasure is not required if the data is necessary for the specified purpose or is required by law (s12(3)), which is a significant loophole.

• To publish in a prescribed manner the business contact information of a Data Protection Officer, or other respondent on behalf of the Data Fiduciary (s8(9)).
• To “establish an effective mechanism to redress the grievances of Data Principals” (s8(10)).

A Data Fiduciary cannot contract out of these obligations by passing them on to a Data Processor that it employs (s8(1)).

The Central Government can designate certain Data Fiduciaries to be Significant Data Fiduciaries (SDFs) who have extra obligations, namely:

• to establish periodic independent audits (including appointing the auditor) to evaluate the SDF’s compliance with the Act; and
• to establish periodic Data Protection Impact Assessments;
• to undertake such other measures as may be prescribed.

SDFs are to be appointed according to such relevant factors as the Central Government may determine, “including the volume and sensitivity of personal data processed; risk to the rights of Data Principals; potential impact on the sovereignty and integrity of India; risk to electoral democracy; security of the State; and public order.” (s10(1)). An SDF need not satisfy any particular combination of these attributes, but they are indicative of the legislative intention. For example, a small organisation might be involved in a mass facial recognitions scheme, or misuse people’s personal data on social media in a way that could influence elections.

An overseas SDF must have a Data Protection Officer based in India, who is the point of contact for grievance-handling and is responsible to the company’s overseas Board of Directors, or have similar seniority (s8(2)(a)).

RIGHTS OF DATA PRINCIPALS

The rights of Data Principals to access, correction, updating deletion etc (ss11-12) apply where the Data Principal has previously consented to the collection of personal data by the Data Fiduciary, and where the data has been voluntarily provided (under s7). There are no such
rights where the personal data has been received from a third party, or extracted from a documentary source, even if this data requires updating or correction. Other rights do not have this restriction.

The rights of Data Principals are:

• To obtain a summary of personal data being processed and the processing activities undertaken ....” (s11(1)(a)).
• To obtain “the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared” (s11(1)(b)), but not in relation to law enforcement.
• To obtain “any other information related to the personal data of such Data Principal and its processing, as may be prescribed” (s11(1)(c)). For example, a right to portability could be prescribed, which the Act does not otherwise provide.
• “The right to correction, completion, updating and erasure.” Erasure must be provided unless the data is necessary for the specified purpose or is required by law (s12(3)).
• “The right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager”. “The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board.” (s13). Responses must be within a prescribed time (s13(2)), vital because otherwise a non-responsive Data Fiduciary could prevent a Data Principal being able to get their complaint before the Board so that it knows about and deals with matters of public importance. Individuals have no right to go direct to the courts.
• “The right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal” (s14). Data privacy rights can survive death, but only it seems if the right to nominate a post-mortem representative is exercised, since it does not go automatically to a person’s heir if there is no nomination. No time limit is stated.

The Data Protection Board

A Data Protection Board of India (DPB) is created by the Act with a Chairperson and an unspecified number of Members appointed by the Central Government for (renewable) two-year terms (s18-20). It “shall function as an independent body” (s28(1)) and is a body corporate that can sue or be sued (s28(2)). It does have some other indicia of independence as well, such as limited grounds for removal from office, a right of its Members to be heard (s21), and a prohibition on post-office employment (s22).

However, other factors mitigate against effective independence. Two years is too short a term of appointment for DPB Members to show independence (five years is normal), because the Central Government will always hold over them the threat of imminent non-reappointment. The Board’s powers could be constrained by requirements for their exercise being prescribed (s28(7)(d)). Budget and staffing are under the control of the Government (s24). Whether the Board would be assessed as independent is uncertain, but this may not matter to it (EU adequacy may no longer be a live issue, and questions of constitutionality may never arise).

The Board has powers to investigate data breaches and complaints against Data Fiduciaries (and others), to “impose penalties” (s27(1)), and to “issue such directions as it shall consider necessary” (s27(2)), and to “take action in accordance with the provisions of this Act” (s28(2)). It is unclear what this last adds. It has no power to investigate matters of its own volition.

In effect, there is a right of re-hearing by the Board (perhaps the whole Board) for businesses affected by any penalties or directions, after which hearing it may change its order (s27(3)). There is also a right of appeal to the Appellate Tribunal (Telecom Dispute Settlement and Appellate Tribunal13) within 60 days (s29). The TDSAT is regarded as already overloaded. Data Principals have no such appeal rights.

Penalties and compensation

The Board can impose a monetary penalty “specified in the Schedule” for a “significant” breach of the Act (s33(1)). GDPR-like matters specified are to be considered (s33(2)). The maximum penalty for breaches of the Act, for failing to take reasonable security safeguards to prevent data breaches, is equivalent to US$31M (Schedule, item 1). Other breaches carrying potential maximum penalties over US$15M are for failure to notify the Board or affected Data Principals of data breaches, breaches of additional obligations to children, and breaches of additional duties of SDFs (Schedule, items 2-4). Breaches by Data Fiduciaries of any other provisions of the Act or Rules can attract maximum penalties of equivalent to US$6M, which may be too low to deter large-scale breaches of some provisions. The Board therefore has significant powers, often to international standard, to impose penalties on Data Fiduciaries for breaches of the Act, if it chooses to use them.

If the Board imposes two or more fines on a Data Fiduciary, it can recommend to the Government that public access to the Data Fiduciary should be blocked, and intermediaries must comply with such blocking orders (s37). This “censorship” provision may prove controversial.

No civil court may entertain any legal action “in respect of any matter for which the Board is empowered …” (s38), so injunctions against the Board exercising its powers are not possible, and nor are appeals, except to the Appellate Tribunal.

The Board has no powers to order compensation payments to Data Principals, and no court is explicitly granted such power. This is a major deficiency of the Act, compared with international standards. However, it could be argued that, because the Board is not empowered in relation to matters of compensation, a court would not be blocked by s38 from ordering compensation if it otherwise had powers to do so (for breach of statutory duty, breach of confidence, negligence etc.). This is speculative, but worth considering.

Regional Considerations

India’s South Asian neighbours may be affected by India finally having a law, and by its content. Sri Lanka already has a law,14 Pakistan’s Bill (recently agreed to by Cabinet, but not yet introduced to Parliament15), and Bangladesh’s Bill...
might be amended before enactment. These are the last significant countries in Asia not to have a data privacy law, the remainder being authoritarian dictatorships, a hereditary autocracy, or very small democracies. For most practical purposes, all of Asia will soon be a region of data privacy laws.

**Comparing Rights and Obligations with the GDPR**

Considering both these rights and also the obligations of data fiduciaries, they are quite limited compared with the EU GDPR, because they omit the following 12 rights or obligations:

1. additional protections for defined sensitive data (including biometric and genetic data);
2. data portability;
3. limits on automated decision-making;
4. restrictions on data exports;
5. data protection by design and default;
6. direct liability for processors;
7. proportionality in processing;
8. the “right to be forgotten”;
9. DPA cooperation in complaint resolution;
10. representative actions before the DPA or courts;
11. maximum fines based on global turnover; and
12. compensation as a judicial remedy.

To note this is not to suggest that India’s law should include all of these rights or obligations. However, they have become the “gold standard” for international data privacy protection, and for such an important law as that of India to contain comparatively few of these principles has to be regarded as a setback for the advance of global privacy standards.

**The Constitutional Right of Privacy: Is it Met?**

An unusual nine judge “constitution bench” of India’s Supreme Court unanimously decided in *Puttaswamy v Union of India* on 24 August 2017 that India’s Constitution recognises an inalienable and inherent right of privacy as a fundamental constitutional right.

Although privacy is not explicitly mentioned in the Constitution, this case holds that it is implied by Article 21’s provision that “[n]o person shall be deprived of his life or personal liberty except according to procedure established by law” (and is also protected by other constitutional provisions providing procedural guarantees).

Privacy is a subset of liberty. Privacy is not an absolute right, but “[a]n invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.” The Court identified three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice. Most aspects of data protection therefore come within the constitutional protection of privacy.

Subsequent smaller constitution benches of the Supreme Court may now decide the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy. This may include the Digital Personal Data Protection Act, 2023, if a suitable case is brought before the Court. Whether this Act satisfies these requirements is unknown but is certainly debatable. The proportionality of exemptions is one of the most obvious grounds for challenge, and the lack of any principled restrictions on data exports might be another. As detailed above, there are a dozen ways in which India’s law falls short of the GDPR’s standards, and some might become part of an argument about constitutionality. Whether an Indian NGO will challenge the Act, or the current Court, now led by Chandra-chud CJ, will be willing to fully apply the Constitution (both of which occurred in *Puttaswamy*) it is too early to say but should not be disregarded.

**Conclusions: An Act to Benefit Business and Government**

First, it is too early to be sure about some benefits, because so many key factors await future government decisions. For example, which state instrumentalities, and which classes of Data Fiduciaries, will be exempted? Which companies will be designated as Significant Data Fiduciaries? Will the Board recommend that the Government issues “blocking orders” against some companies? Which countries (if any) will be on the data export blacklist? More than twenty matters are “as may be prescribed”.

The answers to these questions will put a very different complexion on the Act.

For businesses based in India (Data Fiduciaries), they now have a “business friendly” Act imposing minimum obligations on them, although with some risks of substantial penalties for breaches.

For foreign businesses, based outside India (Data Fiduciaries) but wishing to outsource processing to India, or to remotely use personal data of persons located in India, or to import personal data from India, the position is mixed. The India Government may prohibit exports to any countries it chooses (or none), and it already has a raft of specific “data localisation” laws. Processing overseas of data on those in India for transactions offering goods or services (including marketing) must comply in full with the Indian Act, but not for other purposes such as monitoring for political surveillance, or for training AI models.

Foreign businesses’ outsourced processing in India is exempt from the Indian Act, but that is not the whole story. EU companies will need to rely on Standard Contractual Clauses and hope they do not have to face a Schrems-like challenge.

Outsourcers from countries like the US with no data export restrictions will have no problems.

For Indian Governments and their instrumentalities (Data Fiduciaries), all are prima facie bound by the Act but benefit from a wide range of complete and partial exemptions from its provisions (with more to come), to an extent that the Act often seems like a blueprint for surveillance of citizens which, while not explicitly allowed at present, is not clearly illegal either.

For Data Principals – data subjects, consumers and citizens – this law provides at best a minimal set of rights and protections by international standards (far fewer than in the EU GDPR), riddled with deficiencies. Sensitive data is not given any extra protection, except for children. Personal data already made publicly available, including on social media or under a legal obligation, is not protected. Nor is data extracted from a documentary source. Very broad government powers to notify exemptions from the Act, both complete and partial, further reduces its scope, and risk authorising comprehensive government surveillance. Until and unless prohibited, personal data can be exported from India to anywhere in the world, with no protections required. “Legitimate uses”
allow personal data to be processed without consent on very broad grounds that have no necessary connection with the original purpose of collection, including expanding State surveillance. Some protections that do exist have crippling exemptions, for example the right of erasure. The Data Protection Board has questionable independence. Its power to fine is insignificant, but whether the actual penalties imposed by the Board will be more than a slap on the wrist for companies, or will ever involve forbidding government intrusions, remains to be seen. It has no power to award compensation. Individuals cannot enforce the Act directly through the courts. Overall, this Act comprehensively fails Indian citizens and consumers.

However, all categories of Data Fiduciaries should restrain their enthusiasm for such a “business friendly” and “government friendly” Act, at least temporarily. There are still hurdles that may need to be overcome. The most substantial might be the decision of India’s Supreme Court in Puttaswamy. If the constitutional requirements it sets out for protection of privacy (including data protection), implied by India’s Constitution, become a means of interpreting this law, it could upset any of the protections given to the various classes of data fiduciaries discussed above.

With a national election soon, this “business friendly” Act is no doubt convenient for Prime Minister, Narendra Modi’s “backsliding democracy”. How strong it will be in advancing the interests of each of these parties – and of India’s overall national interests – will take some time to play out.

REFERENCES

1. Digital Personal Data Protection Act, 2023

2. ‘Government may give six months to industry to align with data protection rules: MoS IT Rajeev Chandrasekhar Economic Times, 5 September 2023

3. The main stages in this evolution were: report by a Committee of Experts on Data Protection (Sikirksna Report), July 2018; Personal Data Protection Bill, 2019 to Lok Sabha, Dec 2019; Bill reported on by a Joint Parliamentary Committee, Dec 2022; Bill withdrawn, August 2022; Nov 2022, new Draft Bill released for public consultation; August 2023, Digital Personal Data Protection Bill, 2023 introduced in Parliament.

4. PRS Legislative Research (Summary) Digital Personal Data Protection Act, 2023 opm.india.org/billtrack/digital-personal-data-protection-bill-2023 includes a comparison of reports and bills from 2018 which demonstrates how previous versions were stronger.

5. Article 12, Constitution of India: The State includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India.


7. In India, exemptions made by Government delegation are only subject to Parliamentary disallowance if they are ‘specified’. Other forms of delegation, such as by matters being ‘prescribed’ (usually Rules) are not disallowable but only require tabling in Parliament. Matters that may be ‘notified’ are not disallowable.

8. For example, in China, Russia, Kazakhstan, and Sri Lanka (public sector).

9. The following is paraphrased from Ravi Singhania ‘All about Data localisation in India’ Singhania & Partners LLP. April 2023

10. ibid, the RBI clarified what kinds of information must be kept in India in ‘Storage of Payment System Data’ m.rbi.org.inScripts/FAQView.aspx?id=130

11. “Consent Manager” means a person registered with the Board, who acts as a single point of contact to enable Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform; ‘(s2(g)). Another class of consent managers, Account Aggregators (AAs) are already operational in the financial sector.

12. PRS Legislative Research, op cit.

13. Telecom Dispute Settlement and Appellate Tribunal tdsat.gov.in/Delhi/Delhi.php


17. Afghanistan, Cambodia, Laos, Myanmar, and North Korea.

18. Brunei


21. Puttaswamy v UoP, per Chandrachud J at p. 262: From this 547-page decision, the most comprehensive judgment 265 pages is that of Justice Chandrachud, in which Chief Justice Khehar and Justice Agrawal joined, and the other six Justices agreed. Quotes here are from the judgment of Chandrachud, J.

22. The Court held that privacy’s constitutional protection ‘emerges primarily from the guarantees of life and personal liberty in Article 21’ and that ‘[e]lements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III’. Puttaswamy v UoP, per Chandrachud J at p. 262.

23. The relationships between privacy and liberty were stated by Justice Chandrachud to be that '[p]rivacy constitutes the foundations of all liberty because it is in privacy that the individual can decide how liberty is best exercised', although '[l]iberty has a broader meaning of which privacy is a subset’. Puttaswamy v UoP, per Chandrachud J at p. 243.

24. Puttaswamy v UoP, per Chandrachud J at p. 262; and see pp. 254-7.


Graham Greenleaf is Professor of Law & Information Systems at UNSW Sydney and Asia-Pacific Editor of PL&B International Report. Valuable comments concerning this article have been received from Malavika Raghavan (LSE), David Erdos (University of Cambridge), Anubhuti Singh (Dvora Research), Ralf Sauer (European Commission), Shohini Sengupta (Jindal Global University), and Elizabeth Coomes (University of Malta), but all responsibility for content remains with the author.
In particular, transatlantic data flows are among the most important for both Europe and the US – there are more data flows between these two regions than anywhere else in the world. Estimates suggest that they are worth about $7.1 trillion, playing a critical role in the EU-US economic relationship.

The new EU-US Data Privacy Framework (Framework) is intended to facilitate such data flows from the EU to the US. These have become increasingly problematic following the Court of Justice of the European Union (CJEU)’s ruling in Schrems II, which invalidated the EU-US Privacy Shield, a mechanism to enable personal data to be transferred to the US without additional safeguards.

Nearly two years after this ruling, following a number of additional safeguards offered by the US government, the European Commission (Commission) concluded again that the US legislation ensures an adequate level of protection for personal data transferred from the EU to organisations in the US for the purposes of Article 45 of the General Data Protection Regulation (GDPR).

The Framework has been welcomed by companies looking for legal certainty for transatlantic data transfers. However, in light of the previous Schrems rulings and the legal challenge recently filed with the CJEU (more on that below), this enthusiasm might be short-lived – it remains to be seen whether the Framework will be upheld by the Court this time. Until then, many companies transferring personal data to the US are likely to continue to take a “belt and braces” approach by using both the Framework and standard contractual clauses.

In this article, we analyse the Framework in detail and consider its practical implications for organisations.

**Adequacy decisions under the GDPR**

The GDPR imposes restrictions on the transfer of personal data to third countries that have not been recognised as providing an adequate level of protection for personal data. Such restrictions are designed to ensure that personal data that is protected under the GDPR will continue to benefit from an essentially equivalent standard of protection in countries to which the data is exported.

The GDPR provides different mechanisms to enable organisations to lawfully transfer personal data to a third country. These include adequacy decisions by the Commission, such as on the Framework. In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards, including the standard contractual clauses approved by the Commission, binding corporate rules in the case of a group of undertakings, or an approved code of conduct or certification mechanism.

When assessing the adequacy of the level of protection, the Commission considers elements such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence of a data protection authority and binding commitments entered into by the country in respect of data protection.

**The former Privacy Shield**

The Commission adopted its adequacy decision on the EU-US Privacy Shield on 12 July 2016, providing a framework and legal basis for EU-US personal data transfers.

Following a complaint filed by Mr Maximilian Schrem and reference for a preliminary ruling by the High Court of Ireland, the CJEU ruled that the Privacy Shield does not ensure adequate protection of personal data, as required by the EU Charter of Fundamental Rights, and is therefore invalid. In particular, the CJEU considered that:

- US surveillance law, *inter alia*, Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, does not contain sufficient safeguards to ensure proportionate use; and
- The Privacy Shield Ombudsperson mechanism introduced by the US authorities to protect EU citizens’ rights does not provide an effective remedy as required by Article 47 of the EU Charter of Fundamental Rights. This is because the Ombudsperson does not seem to have the power to adopt decisions that are binding on US intelligence services, and there are no legal safeguards that would accompany the US political commitment on which data subjects could rely.

Nearly two years after this ruling, the EU and US announced that they had reached a new agreement on the Framework as a replacement for the Privacy Shield. According to the Commission, the Framework addresses the aforementioned concerns raised by the CJEU and introduces significant improvements compared to the previous Privacy Shield.

**Enhancing safeguards for US signals intelligence activities**

The main change made by the US has been Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities, signed by President Joe Biden on 7 October 2022.

To address the concerns raised by the CJEU, Executive Order 14086 provides for additional safeguards for US signals intelligence activities, mainly:

1. **Limiting access to EU data by US intelligence services.** Executive Order 14086 requires that signal intelligence activities be necessary and proportionate and only for the purpose of certain specific legitimate national security and/or intelligence objectives. Executive Order 14086 allows bulk collection but only for a narrower subset of legitimate national security and/or intelligence objectives. It also requires that targeted collection be prioritised whenever possible.

2. **Establishing additional oversight and independent review mechanisms to provide EU individuals with limited redress.** Executive Order 14086 introduces an independent and impartial redress mechanism, including establishing a Civil Liberties Protection Officer and a Data Protection Review Court (DPRC). The former is responsible for ensuring compliance by US intelligence agencies with privacy and fundamental rights. The latter will independently investigate, handle and resolve complaints regarding the collection of EU individuals’ data for national security purposes, including by adopting binding remedial measures. For
instance, where the DPRC finds that data was collected in violation of the new safeguards, it will be empowered to order deletion of the data.

While such “substantial improvements” were welcomed by the European Data Protection Board, the latter expressed concerns about, among others, certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the redress mechanism.6

Similarly, the European Parliament had taken the view that the Framework “fails to create essential equivalence in the level of protection” and adopted a non-binding resolution urging the Commission not to endorse the Framework on 11 May 2023.7 Nonetheless, the Commission still issued a decision approving the Framework on 10 July 2023.

THE FRAMEWORK PRINCIPLES
To join the Framework, US companies must self-certify and commit to a set of seven binding privacy principles (and 16 equally binding supplemental ones) (Framework Principles), as follows8:

1. The Notice Principle – organisations must inform individuals about their participation in the Framework, the types of personal data collected, and any subsidiaries of the organisation adhering to the Principles, among other things.

2. The Choice Principle – organisations must offer data subjects the opportunity to opt out if their personal data is to be (i) disclosed to a third party or (ii) used for a purpose that is materially different from the purpose(s) for which it was originally collected. When sensitive data is involved, opt-in consent is required before the data may be shared with a third party or used for a new purpose.

3. The Accountability for Onward Transfer Principle – where an onward transfer occurs, the controller remains accountable for processing of the personal data and must ascertain that the third party provides at least the same level of privacy protection as is required by these principles.

4. The Security Principle – organisations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorised access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. The Data Integrity and Purpose Limitation Principle – organisations must take reasonable steps to ensure that (i) processing is limited to the purposes for which it was collected, (ii) personal data is reliable for its intended use, accurate, complete, and current, and (iii) they only retain personal data for as long as needed for the purpose of collection.

6. The Access Principle – data subjects must have access to their personal data and be able to correct, amend, or delete that data where it is inaccurate or has been processed in violation of these principles.

7. The Recourse, Enforcement and Liability Principle – this enables effective legal protection and recourse for individuals and sets out consequences to organisations for non-compliance, and compliance verification.

REQUIREMENTS FOR US ORGANISATIONS
The Framework is administered by the International Trade Administration (ITA) within the US Department of Commerce (DOC). To participate in the Framework, US-based organisations are required to self-certify to the ITA via the DOC’s Framework program website and publicly commit to comply with the Framework Principles discussed above.9

While participation in the Framework is voluntary, upon self-certification effective compliance is compulsory. Accordingly, once such an organisation self-certifies to the ITA and publicly declares its commitment to adhere to the Framework Principles, that commitment will be enforceable under US law.

The ITA has implemented a cost recovery program to support the operation of the Framework, which requires that US organisations pay an annual fee to the ITA in order to participate in the Framework.10 The annual fee is tiered based on the organisation’s annual revenue.

Organisations that self-certified their commitment to comply with the Privacy Shield and wish to join the Framework must comply with the Framework Principles. Such compliance includes updating their privacy policies to, among other things, refer instead to their commitment to comply with the “EU-US Data Privacy Framework Principles”.11

Thus, when relying on the Framework, it would be recommended that EU data exporters verify prior to the transfer whether the data importer is actually certified on the DOC’s Framework website and has updated its privacy policy. They may also consider imposing contractual obligations on importers to remain self-certified, comply with the Framework Principles, and flow such obligations down to other third party recipients in case of onward transfers.

PRACTICAL IMPLICATIONS
An Additional Mechanism to Transfer Data to the US: As discussed above, the GDPR provides for a number of mechanisms to enable organisations to lawfully transfer personal data to a third country. At a practical level, the Framework adds to these existing mechanisms and offers, in principle, an attractive alternative for transfers to the US.

This is mainly because, unlike other traditional mechanisms that require the parties to undertake certain formalities, the Framework is more streamlined. It eliminates the burdensome requirements of conducting transfer impact assessments, as further discussed below, and putting in place a sometimes complex web of agreements including standard contractual clauses. Yet, it has the same legal effect as the traditional safeguards.

Consequently, it seems like the Framework has everything needed to be popular amongst EU data exporters when transferring data to the US. But the reality is rather more complex.

Limited scope of the Framework: The Framework has a limited scope. First, it only applies to US companies that have joined and been certified under the Framework. As of the date of this article, approximately 2,500 US
companies have self-certified on the DOC’s Framework program website. This is less than half of the 5,380 companies that were participating in the previous Privacy Shield at the time of the Schrems II ruling. It is true that the Framework has only been around for two months (compared to four years as for the Privacy Shield), but also some US companies have adopted a “wait-and-see” approach and are reluctant to sign up to the new Framework due to the legal uncertainty around it.

Second, as with the previous Privacy Shield, only those companies subject to the jurisdiction of the Federal Trade Commission (FTC) or the US Department of Transportation (DOT) are eligible to self-certify their compliance with the Framework. Accordingly, companies such as banks, insurance and telecommunications companies are unable to participate in the Framework.

Third, the Framework only covers data transfers from a public or private entity in the EEA to the US. As for the United Kingdom, an extension to the Framework to cover transfers of personal data from the UK has been agreed in principle. [A UK-US data agreement has now been announced to commence on 12 October 2023.] Accordingly, multinational companies that transfer personal data to other third countries without a corresponding adequacy decision, such as China and India, must continue to rely on the traditional transfer mechanisms for such data transfers under the GDPR. It seems that the standard contractual clauses and transfer impact assessments won’t go away any time soon.

Need for Transfer Impact Assessments? One of the most significant practical consequences of the Schrems II ruling was that organisations must carry out transfer impact assessments (TIAs) when transferring personal data outside of the EEA.

This means that the data exporter (in collaboration with the importer, where applicable) must assess “on a case-by-case basis” whether the law of the third country ensures adequate protection of personal data under the GDPR (e.g. because of potential access by law enforcement or national security agencies). Depending on the outcome, the exporter must consider whether supplementary technical, contractual and organisational measures are necessary to achieve such level of protection.

The Framework has a bearing on the TIAs. A TIA is not needed when making a transfer under the Framework, but is still needed for transfers under the standard contractual clauses.

Nevertheless, in our view, the Commission’s comprehensive adequacy assessment should allow organisations to rely on that assessment when conducting TIAs for transfers of personal data to the US. The Commission’s assessment in effect creates a presumption that the TIA will be satisfied, as the safeguards that have been adopted by the US Government under Executive Order 14086, as discussed above, apply to all data transfers to US companies, regardless of the transfer mechanism used.

In light of these changes introduced under the Framework, data exporters may also need to revise and update their previously performed TIAs.

**Heading for Schrems III (or Rather Latombe I)?**

Reactions to the adoption of the Framework on 10 July 2023 have not been slow in coming.

As expected, NOYB announced that it will challenge the Framework within 24 hours of its adoption, arguing that it is “largely a copy of the failed Privacy Shield” and that “the fundamental problem with FISA 702 was not addressed by the US”.

While all eyes were on Mr Schrems, on 6 September 2023 Mr Philippe Latombe, a French Member of the European Parliament, brought (in his own name) an action for annulment of the Framework before the CJEU under Article 263 of the Treaty on the Functioning of the European Union (TFEU). This has taken place within less than two months of the adoption of the Framework, which is the time limit for bringing such legal actions under EU law.

In his claim, Mr Latombe argues that the Framework violates the EU Charter of Fundamental Rights and the GDPR, due to insufficient guarantees of respect for privacy in relation to bulk collection of personal data. It is unclear when a judgment on the proceedings will be handed down. The average time taken by the General Court (GC), which is competent to hear actions for annulment in the first instance (with some exceptions), to deal with cases closed by judgment amounted to 20.4 months in 2022. In comparison, the Schrems II ruling rendered by the Grand Chamber in a preliminary ruling has taken 26 months.

We can therefore expect that the uncertainty around the validity of the Framework will remain for approximately two years.

Also, once the GC hands down a judgment, the parties may still appeal to the Court of Justice (limited to points of law), which will decide the case in the second and last instance. Such an appeal could further delay the final judgment.

Nevertheless, Mr Latombe also requested the suspension of the Framework through interim measures. The applicant must demonstrate that the measures are urgent and that without them he would suffer serious and irreparable harm. If awarded, such interim measures could immediately suspend the effects of the Framework, rendering all transfers of personal data to thousands of Framework-certified US companies potentially unlawful (unless they are also backed by the standard contractual clauses).

As a result, until the Framework is reviewed and upheld by the CJEU, thousands of European companies transferring personal data to the US are likely to continue to take a “belt and braces” approach by using both the standard contractual clauses and the Framework.

**Author**

Ceyhun Pehlivan is Counsel at Linklaters and co-lead of the Telecommunications, Media and Technology and IP Practice group in the Madrid office, and Adjunct Professor at IE Law School. Email: ceyhun.pehlivan@linklaters.com

**Information**

The opinions expressed in this article are those of the author. This article is for general information purposes and is not intended to be and should not be taken as legal advice.
The UK-US Data Bridge was announced by the UK’s Department for Science, Innovation and Technology (DSIT) on 21 September and is due to enter into force on 12 October. If companies meet certain conditions, they will be able to transfer personal data to the US without using legal safeguards, such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs). This UK-US instrument follows the recently adopted EU-US version.

Behind this headline news, lie 16 explanatory documents from DSIT, the UK Information Commissioner (ICO), and several from the US, including the Federal Trade Commission (FTC), the International Trade Administration, the Director of National Intelligence and the Department of Transportation.

UK-based companies planning to send personal data to the US using this Data Privacy Framework (DPF) must check whether the recipient companies have self-certified to conform with privacy principles enforced by the FTC and Department of Transportation (DoT), and administered by the Department of Commerce (DoC). “The Data Privacy Framework includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for organisations to be able to join the DPF. These principles take the form of commitments to data protection and govern how an organisation uses, collects and discloses personal data.”

**EXCEPTIONS AND RESERVATIONS**
US organisations not subject to the jurisdiction of either the FTC or DoT — for example, banking, insurance, and telecommunications companies — are not included in the scheme.

DSIT acknowledges that the DPF does not mirror exactly the definition of special category data in Article 9(1) UK GDPR, as it does not include genetic data, biometric data for the purpose of data concerning sexual orientation. If an organisation cannot rely on the DPF, then it should continue to use existing provisions, such as BCRs and SCCs. Companies may also need to carry out a transfer risk assessment to validate their transfers.

The ICO was consulted on the Data Privacy Framework and expressed reservations about the scheme stating “there are four specific areas that could pose some risks to UK data subjects if the protections identified are not properly applied. They include:

1. “The definition of ‘sensitive information’ under the UK Extension does not specify all the categories listed in Article 9 of the UK GDPR…there is no current requirement for UK organisations to identify information as sensitive. This creates a risk that the protections may not be applied in practice.”

2. “For criminal offence data, there may be some risks even where this is identified as sensitive because, as far as we are aware, there are no equivalent protections to those set out in the UK’s Rehabilitation of Offenders Act 1974.”

3. “The UK Extension does not contain a substantially similar right to the UK GDPR in protecting individuals from being subject to decisions based solely on automated processing which would produce legal effects or be similarly significant to an individual. In particular, the UK Extension does not provide for the right to obtain a review of an automated decision by a human.”

4. “The UK Extension contains neither a substantially similar right to the UK GDPR’s right to be forgotten nor an unconditional right to withdraw consent.”

The ICO also highlighted specific areas which the Secretary of State should monitor before a formal review in four years’ time.

Saudi Arabia’s data protection law enters into force

The final Implementing Regulations are generally business-friendly and bring the law closer to the EU GDPR. By Brian Meenagh and Lucy Tucker of Latham & Watkins.

The Saudi Data & AI Authority (SDAIA) recently issued the final Implementing and Transfer Regulations for the upcoming Personal Data Protection Law (PDPL), the first comprehensive data protection law in Saudi Arabia. This follows the publication of consultation drafts of the Implementing and Transfer Regulations in April 2023 (the Consultation Draft). The PDPL was issued under Royal Decree No. M/19 on 16 September 2021, and amended pursuant to Royal Decree No. M/148 on 27 March 2023.

The PDPL came into force on 14 September 2023; however, we do not expect enforcement activities until mid-September 2024 because its preambles include an additional one-year transition compliance period.

The PDPL has a wide extra-territorial scope and will apply to any processing of personal data that takes place in the Kingdom, and to the processing of personal data of individuals located in the Kingdom by organisations outside of the Kingdom. SDAIA will be the initial competent authority to enforce the PDPL.

Penalties for non-compliance with the PDPL include the following:

- Fines of up to 5 million Riyals (approximately $1.3 million), which may be doubled for repeat violations.
- Possible imprisonment for up to two years for certain disclosures of sensitive personal data in violation of the PDPL, if the discloser intended to harm the data subject or achieve personal benefit. Possible imprisonment represents a serious risk to doing business in Saudi Arabia. It is uncertain which individuals may be subject to imprisonment if a legal entity is responsible for the violation.
- Warnings.
- SDAIA has the right to “seize the means or tools used in committing a violation” until a decision is made, and a competent court may also order the “confiscation of funds obtained as a result of committing the violations”.
- A party which suffers “material or moral damage” as a result of a violation may apply to a competent court for proportionate compensation.

With the exception of a couple of outliers (see legal basis comments below), the updates to the Implementing Regulations are generally business-friendly and bring the PDPL closer towards the requirements of the EU General Data Protection Regulation (GDPR).

We have included below some high-level comments on key topics in the PDPL and Implementing Regulations, with a focus on areas which deviate from the GDPR or which have recently been updated in the final Implementing Regulations.

KEY TOPICS

PDPL and Implementing Regulations:

- Legal basis and disclosing personal data: The final Implementing Regulations do not contain overarching legal basis wording from the Consultation Draft, which provided a list of a common legal basis which may be relied on for various types of processing under the PDPL. The legal basis wording under the PDPL is fragmented. Separate legal basis requirements apply for processing personal data more generally and for disclosing personal data, which appears to be treated differently from a legal basis perspective.

- Data subject rights: Unlike in the Consultation Draft, the application of data subject rights (e.g. access, rectification, restriction, erasure) are not limited to a certain legal basis for processing. Controllers have 30 days to action requests, and may extend this period by up to an additional 30 days in limited circumstances. The right to data portability is not included. In addition, if a controller becomes aware that personal data is inaccurate, outdated or incomplete, it must rectify this without delay. Controllers will need to implement procedures and tools for recognising and responding to subject rights requests.

- Transparency: Controllers must provide data subjects with privacy notices setting out details of the personal data processing, either before or while collecting their personal data. If the controller receives personal data from an individual other than the data subject, the controller has 30 days to provide the data subject with the privacy notice. Additional transparency information must be provided for certain processing, including the adoption of new technologies or making automated decisions based on personal data.

- Consent: A high threshold for consent is applied. Similar to the GDPR, consent must be freely given, specific and clear, and separate consents must be obtained for each processing purpose. Controllers must document consent. Explicit consent must be obtained if the processing involves sensitive or credit data, or if automated decision-making is carried out. Data subjects must be able to easily withdraw consent.

- Children’s data: Provisions are included on legal guardians acting on behalf of individuals who lack full capacity. In the Consultation Draft, parental consent was generally not required for processing personal data of children aged 13-18. This wording has been removed from the final version; at what age children will be considered to have capacity to provide consent for the processing of their personal data is now unclear.
• **Legitimate interests**: Further details are provided on the legitimate interests legal basis, and the wording now more closely aligns with legitimate interests under the GDPR, with a balancing test between the interests of the controller and the rights and interests of the data subjects. Controllers must carry out a legitimate interest assessment before relying on legitimate interests. Legitimate interest cannot be relied on for processing sensitive data.

• **Data processors**: Mandatory contractual terms apply to data processing agreements, which are similar to the GDPR requirements, although less detailed. In addition, controllers must periodically assess a processor’s compliance with the PDPL and Implementing Regulations.

• **Data security**: Controllers must comply with relevant controls issued by the National Cybersecurity Authority (NCA), or recognised best practices if the controller is not subject to NCA controls. Non-compliance with the applicable NCA controls might therefore put controllers at risk of SDAIA enforcement action under the PDPL, as well as any NCA enforcement.

• **Breach notification**: Controllers must notify SDAIA within 72 hours (and relevant data subjects without undue delay) of becoming aware of a personal data breach, if the breach may cause harm to personal data or the data subject. There is no specific risk threshold (e.g. no reference to the likelihood or severity of the harm).

• **Data Protection Impact Assessments (DPIAs)**: Controllers must carry out risk assessments of certain processing activities, including the processing of sensitive personal data (seemingly even if not large-scale), collecting or combining data sets from different sources, the continuous and large-scale processing of personal data relating to children or others who lack capacity, continuous monitoring of data subjects, processing using new technologies, making decisions based on automated processing, or providing a product or service that involved processing likely to cause serious harm to data subjects. The risk threshold for carrying out a DPIA appears lower than under the GDPR. Controllers must provide a copy of the DPIA to any processor acting on their behalf in relation to the processing, which may impact trade secrets and confidentiality, and is not required by the GDPR.

• **Health and credit data**: Specific requirements apply to the processing of health and credit data.

• **Direct marketing**: Consent appears to be the only legal basis which can be relied on for marketing. However, the consent requirements are a little unclear because of separate articles in the Implementing Regulations on sending advertising materials and direct marketing. The article on sending “advertising or awareness material” states that in the absence of prior interaction between the controller and the recipient, consent is required to send advertising or awareness material. However, the article on “direct marketing” simply states that consent is required to process personal data for direct marketing purposes, without distinguishing situations in which there is an existing relationship between the controller and the recipient. Recipients must be able to easily opt out of receiving marketing. The requirements on direct marketing are without prejudice to the Telecoms and IT Act. Controllers will be required to implement consent mechanisms and provide opt-out mechanisms.

• **Official ID documents**: Controllers may not photograph official ID documents unless requested to do so by a government authority or if required by law.

• **Data Protection Officer (DPO)**: Controllers are required to appoint a DPO in broadly the same cases as under the GDPR (e.g. regular and continuous monitoring of individuals on a large scale, and if the core activities involve processing sensitive data). The final Implementing Regulations set out the responsibilities of the DPO, which are also broadly similar to those under the GDPR. The SDAIA shall issue further rules regarding DPOs; whether DPOs will be required to be independent (as per the GDPR) and whether the DPO could be located outside of the Kingdom is currently not clear.

• **Record of Processing Activities (ROPA)**: Controllers must maintain a record of their processing activities, including for 5 years following the completion of processing activities. The Implementing Regulations contain a list of information which must be included in the ROPA, which mirrors the GDPR requirements. Controllers must provide their ROPA to SDAIA on request.

• **National register of controllers**: Controllers are required to register on a national portal, and SDAIA shall issue rules regarding registration.

• **Data subject complaints**: Data subjects may complain to SDAIA within 90 days of an incident.

• **SDAIA powers**: SDAIA has broad powers to supervise the PDPL’s implementation and monitor compliance. It is not clear what SDAIA’s enforcement priorities will be, including how closely it will monitor the enforcement actions of other regional or international privacy regulators, given the similarities in the PDPL to international privacy laws such as the GDPR. The final Implementing Regulations do not contain any changes or further details on topics such as joint controllers (this concept is still not included) or local representatives (it appears these are not required).

**PDPL and Transfer Regulations**

• **Key update on transfer purposes**: Under the PDPL, controllers may only carry out a transfer of personal data outside of the Kingdom where this takes place for a specified purpose. The key update in the final Implementing Regulations is that additional specified purposes have been introduced, which are business-friendly. These additional specified purposes are:
  - the transfer is for processing operations which enable the controller to carry out their activities, including central management operations;
- the transfer results in the provision of a service or benefit for the data subject; or
- the transfer is to conduct scientific research and studies.
These purposes are in addition to those specified in the PDPL, such as a transfer to perform an obligation to which the data subject is a party. Note that a transfer mechanism is still required in all cases.

- **Data minimisation:** Controllers are required to limit transfers of personal data outside the Kingdom to the minimum data necessary. Any appropriate means can be used for this purpose, including data maps which document the need to transfer the data.

- **Adequacy criteria:** The final Implementing Regulations set out the criteria which the SDAIA will apply (in coordination with other Kingdom authorities) for assessing whether a recipient jurisdiction can be considered adequate, in order to allow data transfers to that jurisdiction. This criteria is broadly similar to the adequacy criteria under the GDPR, with some notable differences, such as the additional consideration of the willingness of the data protection supervisory authority in the recipient jurisdiction to cooperate with the SDAIA.

- **Alternative transfer mechanisms (safeguards):** In the absence of an adequacy decision, the alternative transfer mechanisms appear very similar to the GDPR and include Binding Corporate Rules (BCRs) approved by the SDAIA, Standard Contractual Clauses (in the form to be issued by the SDAIA) and certifications of compliance.

- **Derogations:** In the absence of an adequacy decision or inability to rely on an alternative transfer mechanism, data transfers may take place relying on a derogation, including when the transfer is necessary to perform a contract with the relevant data subject and when the transfer is necessary to protect the vital interests of the data subject. However, unlike the GDPR, there is no derogation available if the data subject provides their consent for the transfer or if the transfer is necessary for legal claims.

- **Restrictions:** Controllers must immediately stop and re-assess the risks of transfers which rely on an alternative transfer mechanism (safeguard) or a derogation if - the transfer impacts national security or the vital interests of the Kingdom,
- a risk assessment identifies that the transfer causes a high risk to the privacy of data subjects, or - safeguards adopted by the controller are no longer applicable or enforceable by the controller.

- **Mandatory risk assessments:** Controllers are required to conduct a risk assessment of transfers which rely on an alternative transfer mechanism (safeguards), derogation, and for any continuous or large-scale transfers of sensitive data outside of the Kingdom (seemingly regardless of whether the recipient jurisdiction is considered adequate).

- **Guidelines:** The SDAIA is required to issue guidelines relating to data transfers.

---

**New Zealand issues Privacy Amendment Bill**

The New Zealand Government’s Privacy Amendment Bill (Bill) would improve transparency for NZ citizens. The Bill would amend the current Privacy Act 2020 by making it an obligation for organisations to inform people why they are collecting personal information and who will be holding it.

“This is fundamental to protecting the privacy rights of individuals by informing them about how their personal information is used,” says the Privacy Commissioner Michael Webster.

“We support the amendment for the Privacy Act to have a broader transparency requirement so that agencies need to think about how to inform people they’re collecting their information, regardless of its source, and what their privacy rights are.”

The amendment would not apply to personal information collected before 1 June 2025.


---

**Korea: amended PIPA enters into force**

The amended Korea Personal Information Protection Act (“PIPA”) and the subsequent Enforcement Decree of the PIPA entered into force on 15 September.

The changes to the PIPA include stronger data subject rights with regard to automated decision-making, and new legal bases for international transfers which are not based on consent. Korea’s DPA is currently working on a revised enforcement decree for some of the provisions of the amended law that will take effect later, including the right to data portability.

- See [www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do](http://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do)

---

**AUTHORS**

Brian Meenagh is a Partner at the Riyadh office, and Lucy Tucker is an Associate at the Dubai office of Latham & Watkins.

Emails: brian.meenagh@lw.com

lucy.tucker@lw.com
Israel aims to retain its EU GDPR adequacy status

Gilad Semama, Head, Israel’s Privacy Protection Authority, told PL&B about the status of the law and how it is implemented. Stewart Dresner reports from Tel Aviv.

Israel’s privacy law dates back to 1981 and much has changed since then. In 2017, amendments to Israel’s privacy law had a focus on data security issues.

On 7 May this year, the government published the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023. They cover the transfer of personal data from the European Economic Area (EEA) to Israel and cover data deletion, retention, accuracy, the duty to inform data subjects about certain types of information, and sensitive data (special category data). These Regulations entered into force on 7 August 2023 for transfers of data from the EEA to Israel on or after this date. They will enter into force within one year of this date for data which is already in Israel on the date of entry into force; and on 1 January 2025 for any other data held in a database in Israel which also contains data that was transferred from the EEA, and for which the Regulations apply.

In addition, the government is promoting amendments to the Protection of Privacy Law with a focus on enhancing the Privacy Protection Authority’s (PPA’s) enforcement powers and to extend Israel’s law to cover or strengthen aspects of the GDPR only partially covered, or not covered, in Israel’s law. They include broadening the current definition of “personal data”, for example, to include any identifiable personal data; data protection by design and default; and the appointment of Data Protection Officers.

Stewart Dresner of PL&B put questions to Semama about other developments in Israel.

PPA PRIORITIES

Since your appointment in November 2021, what have been your priorities?

The Privacy Protection Authority (PPA) aims to strengthen its enforcement actions and to increase compliance with the provisions of the law by all sectors of the economy. In this framework, the Authority formulated an updated operating strategy. This includes, among other things, the obligation to immediately report to the Authority areas of concern or the occurrence of a data breach in any organisation. The PPA’s goal is to provide support to them.

Punishment is not necessarily the main goal of the authorities’ enforcement strategy. However, the PPA will not hesitate to use all sanctions available, especially against those who knowingly violate laws or who do not report to the authority a suspicion of a severe data breach which they are obligated to do by law. Our overarching goal is protecting individuals. This includes enforcement, educating the public, issuing guidelines, policy documents and recommendations on various topics and more.

In 2022, the PPA launched a media campaign focusing on the obligation to immediately notify the Authority regarding data breach incidents in light of their increase. Also, the PPA opened a call centre to encourage enquiries from both the public and other stakeholders engaged with privacy and data security issues.

The PPA is focused on strengthening cooperation with various stakeholders in the economy, including with the public sector, and advises on government projects that raise concerns for privacy and data protection, in order to ensure compliance with the law.

As part of the guidelines published by the PPA, the Authority published a document on privacy and data security in the use of Deepfake technologies – the first of its kind. The document includes an explanation of Deepfake technology and reviews the various privacy and legal aspects related to the use of this technology by users and service providers, as well as recommendations to the public and processors.

The PPA clarified that distribution without consent of a Deepfake photo or video that depicts humiliating content or that concerns a person’s personal life, which may be perceived by the public as authentic, constitutes a violation of privacy. The Authority also stated in the document that companies and database controllers that produce fake content using Deepfake technology must comply with information security regulations. Even fake information that is perceived as authentic personal information is information that must be processed complying with Israel’s privacy law. Any forwarding or further publication of the content (for example, forwarding it through instant messaging apps) can constitute a violation of the Privacy Protection Law.

INDEPENDENCE OF THE PPA TO UPHOLD INDIVIDUALS’ RIGHTS

The PPA has an independent status within the Ministry of Justice. Please give us examples of issues when you have needed to assert this independence?

Indeed, the PPA’s independent status, which existed de facto from its establishment, was recognised formally by the Israeli government in 2022, within Government Resolution No. 1890 “The Independence of the Privacy Protection Authority”. The PPA exercises its powers independently when fulfilling its tasks, including enforcing the Privacy Protection Law’s provisions. For example, the PPA has investigated different political organisations, on a state and municipal level, for data breaches which occurred in a political context.

In addition, the Authority is a prominent participant when the Knesset (the legislature) discusses laws that include provisions that may infringe privacy and data protection. For example, the PPA opposed a bill on facial recognition for police enforcement purposes, due to the fact that the law did not include sufficient mechanisms to protect
human rights and privacy. Eventually this part of the bill was withdrawn by the government.

Your website describes your status as a “civil rights gatekeeper.” Please give examples of how you are performing this function with examples of complaints and how you have responded to them.

The PPA is the gatekeeper of citizens’ rights in the field of data protection, and its main task is to promote compliance with data protection laws in every organisation, business and public body that manages personal information, to ensure that they manage the information in their possession properly in accordance with privacy protection laws and regulations.

The handling of enquiries from the public is a central tool for maintaining contact and communication with them and with anyone who sends enquiries to the PPA. As part of the activities of the public and government relations department, inquiries/complaints are received about violations of the law or regulations, as well as questions on a variety of issues related to privacy protection. The PPA also receives enquiries from professional parties, such as lawyers and data protection experts, regarding the implementation and enforcement of the Privacy Protection Law and its regulations in their day-to-day work.

The complaints or referrals received by the authority are an important source of information for conducting administrative and criminal enforcement actions, and for determining violations of the law in appropriate cases. In addition, the Authority uses enquiries from the public for identifying issues in which regulatory actions are required. The PPA’s responses include guidelines, legal opinions, and questions and answers on various issues.

There are many examples of cases in which complaints received by the PPA have led to enforcement action. Examples are the case of a company’s refusal to allow data subjects access to review information about them, or cases in which data was used contrary to the purpose for which it was collected. In these cases, the Authority contacts these companies and examines whether violations of the law have been committed and, as a result, decides on confirming whether a violation has taken place and imposes sanctions on a case-by-case basis.

**The PPA’s enforcement work**

**How many people work at the PPA?**

There are just over 50 PPA staff. The enforcement department, which is the largest department in the PPA, consists of three sections:

1. **Audits (broad inspection)** – We have developed an audit mechanism which examines sectors and markets. The mechanism enables the PPA with modest resources to examine many organisations. The PPA identifies sectors and markets which pose risks to personal data, and develops questionnaires to be answered by organisations that operate in those markets. Their responses provide the PPA with information regarding the quality and scope of the measures they take to comply with the provisions of the law and regulations. The audit mechanism enables the PPA to identify sectoral failures that require intervention, and to issue instructions to the inspected bodies, as well as to obtain a picture of the sector regarding compliance with the provisions of the law. The publication of the audit findings reports enable us to provide practical guidance for organisations in the sector. The audits are initiated by the Authority and do not depend on third parties’ requests to the PPA.

2. **Administrative investigations** – The PPA conducts hundreds of investigations following complaints referred to the PPA or following intelligence regarding breaches. Administrative investigations are usually reactive, even if sometimes initiated by the PPA. At the end of the investigation, the authority issues administrative fines as well as corrective orders, supervises their implementation and issues decisions regarding infringements when applicable.

3. **Criminal investigations** – The criminal route is available for specific cases which justify the investment of substantial resources required for the conduct of a criminal investigation. These are usually cases with broad implications, or of public importance, and cases in which the damage caused was significant. The basis for opening a criminal investigation is usually intelligence provided by various sources. The investigation begins with undercover actions, at the end of which searches, seizures of computers and computer materials will be carried out and witnesses and suspects will be interrogated. Most of our investigations eventually lead to indictments.

Israel’s PPA has the power to use criminal sanctions. How do you balance your efforts between administrative and criminal sanctions?

The resources at the disposal of the PPA are limited by nature, and therefore require the PPA to focus on enforcement actions that will create the greatest impact on the level of compliance throughout the economy. Enforcement actions against large entities on “softer” issues will usually be handled as an administrative investigation, while the more severe cases will be handled at the criminal level according to the circumstances.

**Data breaches**

What are the provisions in Israel’s current law on data breaches? Do you have a helpline to assist organisations?

Israel’s Data Security Regulations include a breach notification obligation, to notify the PPA of any severe personal data breach (with a very broad definition of the term “severe data breach”). The PPA has opened a call centre where staff receive enquiries on a variety of issues, including data breach notifications. In addition, the PPA launched a media campaign to raise awareness of the obligation to notify the Authority immediately after receiving information about a suspicion of a data breach. The aim is to help organisations from the initial stage of the data breach, reduce the damage to the public’s personal information and limit the damage that the affected organisation might experience.

As part of the campaign, the authority also encourages all stakeholders to contact the hotline on any subject within its jurisdiction.

In addition, the PPA’s enforcement
ANALYSIS

department advises affected organisations from the stage of receiving the data breach notification. The PPA assists them with appropriate preventative measures, as well as measures to reduce the damage, which the EU GDPR describes as “technical and organisational measures.”

Does the PPA publish statistics on the number and type of data breaches, complaints and follow-up actions?

The Authority does not publish statistics regarding data breaches. Information regarding enforcement procedures and public inquiries, is published in the Authority’s annual report. The latest report, published in July 2021, summarises the PPA’s activities in 2019-2020.3

In 2021, the majority of public inquiries focused on data security, data breach notifications, lack of consent, cameras in public spaces and data subjects’ right to access their data.

INNOVATION AND PRIVACY

The PPA has an Innovation and Policy development department. What kind of subjects does this team cover?

The Innovation and Policy Development Department analyses and identifies future trends (technological, social and business practices) and examines their implications for privacy by conducting research and writing innovative privacy policy documents. Also, the department leads the Authority’s strategic planning processes, the field of knowledge and information management within the Authority and promotes the Authority’s positioning in the international arena. The department also promotes and fosters the development of Privacy Enhancing Technologies.

Israel is famous for being “The Start-up Nation” known for its high-tech successful innovations in many fields with research centres for many international companies, such as IBM, Google and Microsoft and many Israeli start-up companies including Waze, acquired by foreign companies. Do you face criticism that your work at the PPA is limiting innovation in high-tech? If so, how do you respond?

The PPA aims to promote privacy and data protection and at the same time to allow innovation. In order to do so the PPA meets with regulators, academics and industry representatives on a regular basis to exchange views.

ISRAEL AS PART OF THE WORLD’S DPA NETWORK

Israel was accepted as an OECD member in 2010. Has this membership had a visible or invisible impact on the PPA or government policy in the privacy field?

The PPA is an active member of the OECD’s privacy institutions. As such, the PPA’s OECD representative is a Bureau member in the OECD’s Working Party on Data Governance and Privacy. The PPA closely follows the OECD’s publications and recommendations on privacy matters, contributes to their drafting process and relies on them, alongside other international sources, in the drafting of its own guidelines. Additionally, the PPA updates privacy law stakeholders in the Israeli government about relevant OECD activities on a regular basis.

Israel’s PPA is a member of the Global Privacy Enforcement Network (GPEN) with Data Protection Authorities from around 55 countries. To what extent has this membership and participation in the global sweeps on specific issues helped your work in Israel?4

The PPA is a member of the GPEN Committee and therefore leads and contributes to its projects. The PPA hosted the GPEN Practitioners Event in June 2018, in Tel Aviv. Joint sweeps (monitoring of national trends on specific subjects) are a good opportunity to identify trends which raise concerns globally, and to share and learn auditing methods from colleagues around the world. Since sweeps are covered by national and international media, it is a good opportunity to raise awareness about the privacy risks being examined during the sweep.5

THE PPA’S INFLUENCE IN ISRAELI SOCIETY

Are you working on guidance for business and consumers on how to interpret the privacy law?

The PPA guides all stakeholders on a regular basis, by issuing guidelines, legal opinions, recommendations and by educational initiatives which include workshops, campaigns and press releases. Educating the public and educating organisations are both imperative to the PPA’s mission to enhance and promote privacy and data protection.

Who do you see as the PPA’s allies in society, for example, specialist academics, consumer and civil rights organisations? Do you have support and opposition among business organisations? If so, on which type of issues?

We are in constant dialogue with all the stakeholders mentioned above. The PPA holds forums for the various sectors of the economy (public, private, municipal authorities, data protection professionals) in order to clarify our policy, legal and organisational obligations, to allow participants to raise questions and problems they face in the field of privacy on an ongoing basis. Also, we hold roundtables to exchange views with the relevant parties (academics, NGO’s, law firms, associations, data protection professionals) from all sectors of the economy and to receive suggestions/insights regarding the issues on which the Authority should focus.

In addition, we participate in conferences and training events organised by various organisations (academia, private sector, public sector, not-for-profit organisations) to raise awareness about data protection among various parties involved in the field as part of their work.

Documents published by the PPA are, for the most part, circulated for public consultation prior to their final publication in order to allow anyone interested to express their position regarding the content of the documents and the implementation of the recommendations listed there.

As part of our various actions at all levels, we are exposed to both positive and supportive reactions as well as suggestions for improvement, and sometimes to positions that contradict the PPA’s position. Each response is considered carefully and sometimes these positions eventually have an impact on the PPA’s policy.
Meta paying a daily penalty in Norway

On 6 September, the Oslo District Court ruled that Meta has to pay a daily fee of one million Norwegian krone (circa €87,000) for not complying with the temporary ban on behavioural marketing by Facebook and Instagram issued by Norway’s Data Protection Authority on 14 July.

Meta had asked the Court to suspend the decision, but the Court agreed with the arguments put forward by the Data Protection Authority in the matter.

“This is a thorough ruling that provides useful clarifications. We are very pleased that the Court agrees with our assessments”, said Head of International Section, Tobias Judin.

The deadline for compliance with the DPA decision was set to 4 August 2023, and Meta’s daily fines have been running since 14 August.

The DPA is now considering bringing the matter to the European Data Protection Board in order to extend the ban EU-wide.


Data transfer report identifies trends

Cross border data flows have become easier in Argentina, Australia, Brazil, China, India, Indonesia, Russia, Saudi Arabia, and the United States, a report by Salesforce reveals.

Its cross border data flows index looks at publicly available indicators to evaluate key regulatory aspects that either restrict or enhance the volume and variety of cross-border data flows across G20 economies. These include consent and data localisation requirements, specific mechanisms for data flows, meeting GDPR adequacy requirements, and participation in the APEC Cross-Border Privacy Rules (CBPR) or similar regional system.

“Japan and the United Kingdom score the highest, followed by Singapore and Australia, and then the United States. These five economies generally have strong regulatory provisions and enablers for cross-border data flows, including explicit provisions allowing for international transfers of personal data.”

The report recommends making trusted data sharing frameworks the default. Members of the G20 and G7 have endorsed Data Free Flow With Trust (DFFT) and incorporated it into numerous international trade agreements. The World Trade Organisation (WTO) is using its principles to guide negotiations over global e-commerce rules, the authors say.


GPA’s International Enforcement Cooperation Working Group gives warning on data scraping

The Global DPA enforcement group warns companies that data scraping may be unlawful. Personal information that is publicly accessible is still subject to data protection and privacy laws in most jurisdictions, the DPAs say. Social media companies and the operators of websites that host publicly accessible personal data have obligations under data protection and privacy laws; mass data scraping incidents that harvest personal information can constitute reportable data breaches in many jurisdictions.

Social media companies have a role to play in enabling users to engage with their services in a privacy protective manner. The DPAs have sent their joint statement directly to Alphabet Inc. (YouTube), ByteDance Ltd (TikTok), Meta Platforms, Inc. (Instagram, Facebook and Threads), Microsoft Corporation (LinkedIn), Sina Corp (Weibo), and X Corp. (X, previously Twitter).

The following members of the GPA’s International Enforcement Cooperation Working Group endorse the statement dated 23 August 2023: Australia, China, UK, Canada, Norway, Switzerland, Colombiad, New Zealand, Morocco, Jersey, Mexico, and Argentina.

Effective AI projects face the ultimate test of trust

Artificial intelligence systems are already being deployed in the private and public sectors. What are the pitfalls and prospects? Tom Cooper reports.

Artificial Intelligence is already in use in at least one Data Protection Authority (DPA) and Finland recently made legal changes to allow automatic decision-making by public bodies. Meanwhile, in business, technology departments are demanding that compliance teams either clear the way or give plain guidelines for deploying AI solutions.

A session at PL&Bs 36th Annual International Conference brought together a DPA head, two data lawyers and a data lawyer turned “data disruptor” to discuss the way forward for public authorities and the private sector.

Anu Talus, speaking her capacity of Data Protection Commissioner, Finland, outlined the legal changes that had been made in her country to allow public authorities to use automated decision-making. The systems themselves are also restricted and cannot learn while in use. “This is a framework for the possibility of automatic decision-making, not learning,” she said.

Human intervention came through a correction request. This can be directed to the same authority responsible for the automated decision. This avoids the need for the heavier burden of an administrative appeal. Talus said she saw potential for automated decision-making in handling breach notifications at the DPC. She said tax authorities in Finland had already used automated decision-making.

WHAT ACTUALLY IS AI?

There was some discussion on the definition of AI. Some form of “autonomy” was important it was agreed. Legally the definition in EU AI Act was seen as “fungible” and could cause problems, later, in the courts.

Allan Millington, Global Data Policy Leader, EY, UK said: “To me I see AI as being something which is autonomous but adapted, having some level of control.” He said his legal career had moved through data protection and into the data office. “In the data office I am looking to disrupt,” he said. They were looking at scalable and automated data compliance.

Millington said a use case for AI might be a system to review contracts. AI projects needed a clear problem statement, a value proposition, clear requirements, and process mapping. It is important to look at the current state of the problem – which might be checking contracts for Standard Contractual Clauses (SCCs), or whether data could be used for benchmarking or AI. “There may be efficiencies of scale if you are able to deploy a tool to read though those contracts and take an inference.” The volume was important to assess the value of automation. “Is it ten, or ten thousand contracts?”

You might have a great idea, but dependencies were often overlooked, he said. The project might highlight wider problems in the organisation. Data quality might be poor. For contracts, there might be no central repository so you would have to build one. “In these types of projects, it means always looking at all the dependencies and looking hard,” he said.

Tom Cooper, Partner, Linklaters, UK, said the UK ICO was already using machine learning tools to analyse emails sent to it and to automatically respond to some of those emails. “This is happening now,” he said. That information came from the ICO’s Freedom of Information team, following a request, he said. But the use was limited to emails to the registration inbox, dealing with change of address. He saw that a positive step that the ICO was using the technology, “because if you use it, it is much easier to understand how to regulate it”.

This is also a good example of an “incremental build-out”, “You can start with that very limited use case. If that works well, you can build and you can build,” Church said.

Giles Pratt, Partner, Freshfields, UK said it will be interesting to see if the DPAs are going to get ahead of the private sector. “I suspect that those here that are in the private sector are being hounded with questions from technology officers telling lawyers to either get out the way or give very clear guidelines as to what they can do,” he said. “We are sensing that sophisticated in-house teams are breaking down the workload in perfect stride. Looking at the inputs,
looking at the models, looking at the outputs, and the risks and opportunities across each of those.” Data privacy was a large part of that. Intellectual property, regulatory issues, anti-trust concerns, ethical and reputational risk all had to be considered too, he said.

‘NUCLEAR WEAPON’

One major risk is that AI models could be blocked based on the idea that they had used data that should not have been used in their creation. “That is something where all of us struggle to see where the technology risk arises,” Pratt said. “Because, although the models will have been trained on certain data, the models don’t necessarily use that data when they are in operation,” he said. In the US the Federal Trade Commission (FTC) has settled several cases on the basis that a model developed using data that should not have been used for that purpose, is effectively blocked.

An example is the 2022 case against Weight Watchers, where data relating to young persons was used in breach of the Children’s Online Privacy Protection Rule (COPPA) and without appropriate parental consent. “The order that flows from that is the model can’t be used,” he said.4

That was the “nuclear weapon,” he said. “You can bet that those who are providing those core foundation models are not going to be able to provide indemnity to that sort of risk.”

TRUST

Talus said that transparency, being able to explain to data subjects in plain language, was always important with an AI system. “That also creates trust for using AI,” she said.

Church said this pointed to a bigger problem in the legal profession. “We talk too much about systems and processes and not enough about people.” The focus should be on the end users and their views on whether a use was acceptable. “If you have a case that is fundamentally unacceptable to the people you are using it with, then that is going to be a problem legally, ethically and practically,” he said.

As an example, more advanced use of AI by data protection authorities, for example to resolve complaints, would be problematic. Complaintants may already be sensitized to excessive or automated processing of their data. “So if you then say I am going to resolve your complaint using a machine, then they are not necessarily going to like that,” Church said.

Church referred to a recent study that surveyed attitudes to the use of AI.5 Use for determining welfare eligibility was marginally positive. “That surprises me.” Speed and reduction in human error and discrimination were seen as AI positives. If you have a large-scale AI project, certainly try and understand what the attitude of end users is to it, and try to understand their concerns, he said. “Trying to address that is really important in making the project a success from an ethical perspective and probably from a legal perspective as well.”

ERRORS

Discussion turned to errors. Pratt said attitudes diverged between human errors and machine errors. Millington said that ultimately any system will have a degree of accuracy. Are you aiming for 100 percent accuracy? “That is one of the challenges you get with AI systems,” Church elaborated: “We seem to accept the fact that humans crash cars and kill people frequently. But we have very little tolerance for driverless cars that kill people, because we expect them to be perfect.”

Talus said that, from a public authority’s perspective, clear responsibility was paramount. “This was at the core of our constitutional debate over whether public authorities can actually use automated decision-making or not.”

REFERENCES

1 Talus was elected as chair of the European Data Protection Board in May but had already agreed to speak at this session in her capacity as head of Finland’s DPC.
2 Finland does not have a constitutional court. Parliament’s Constitutional Law Committee oversees constitutional affairs.
3 The European Parliament’s negotiating text has significantly amended the definition of artificial intelligence which now aligns with the OECD definition of an AI system. “Artificial intelligence system’ (AI system) means a system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.” See www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf
4 The compromise text from the Council reads: ‘Artificial intelligence system’ (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.”
5 For a summary and further links to this case see www.ftc.gov/news-events/news/releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive

INFORMATION

PL&B’s 36th Annual International conference was held at St John’s College Cambridge, 3-5 July 2023. Videos and slides from the sessions are available to registered participants at www.privacylaws.com/events-gateway/events/ic2023/video2023
G7 DPAs define priorities for the coming year

DPAs issue a statement on Generative AI with a view to further work on it, and stress the importance of a global enforcement strategy. By Marc Schlegel of Germany’s Federal DPA.

The Data Protection Authorities (DPAs) of the G7 nations; Canada, France, Germany, Italy, Japan, the United Kingdom, the United States and the European Union, met for the third edition of the G7 DPA Roundtable 20-21 June 2023 in Tokyo.

During the meeting, convened under the chairpersonship of Ms Tanno Mieko, Chairperson of the Personal Information Protection Commission (PPC) Japan, members of the DPAs discussed current key topics of privacy and data protection, including the further development of “Data Free Flow with Trust” (DFFT) and its possible operationalisation as well as emerging technologies and enhancing international enforcement cooperation. For the first time, the Roundtable also adopted a separate paper on the challenges that (generative) AI technologies might pose to data protection and privacy.

**BACKGROUND**

The DPAs of the G7 nations started to meet annually in 2021, following an initiative of the UK Information Commissioner’s Office during the UK’s G7 Presidency. At the inaugural, albeit virtual, Roundtable meeting chaired by the then UK Information Commissioner Ms Elizabeth Denham CBE, the G7 DPAs discussed a number of specific key issues and explored possible areas of closer cooperation. Topics included, inter alia, questions of government access and international data flows, and designing AI in line with data protection. The results and main messages of this first roundtable were summarised in a joint Communiqué.1

The following G7 DPA Roundtable 2022, held in Bonn during the German G7 Presidency and chaired by the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), Professor Ulrich Kelber, deepened discussions on several fundamental regulatory and technological issues and developments in the context of DFFT; e.g. international transfer tools, Privacy Enhancing Technologies (PETs), de-identification of personal data and ethical AI governance. The Communiqué2 issued as a result of the Bonn meeting thus aimed at “promoting DFFT and knowledge sharing about the prospects for International Data Spaces”. Contemplating the future of the group’s efforts, the 2022 Communiqué called on the G7 DPAs to engage in further discussions at expert level with the aim of developing an action plan and work towards tangible outcomes under the 2023 chair provided by Japan’s PPC.

This year, the group’s collaboration was guided by three pillars, each of which was the topic of a dedicated working group: (1) DFFT, (2) Emerging Technologies and (3) Enforcement Cooperation.

**DATA FREE FLOW WITH TRUST (DFFT)**

In their Communiqué3 adopted at the 2023 Tokyo meeting, the G7 DPAs recognised the benefits that may arise from cross-border transfers of data but highlighted that, at the same time, such transfers can raise serious challenges to the protection of personal data and privacy. They therefore stressed that within the concept of DFFT, “trust” is a vital component and that a high standard of data protection is a fundamental requirement and prerequisite to facilitate the free flow of data.

To this end, the DPAs reaffirmed their commitment to work towards identifying commonalities and elements of convergence between existing regulatory approaches and instruments for data transfers in order to foster future interoperability, where possible, and to facilitate safe cross-border transfers of personal information.

The DPAs also expressed their support for the efforts made in various international fora regarding DFFT and encourage their further development, notably:

- the ongoing work undertaken by the “Global Frameworks and Standards Working Group” of the Global Privacy Assembly (GPA) on the comparison of model contractual clauses;
- the work of the “Working Party of Data Governance and Privacy in the Digital Economy” of the Organisation for Economic Cooperation and Development (OECD); and
- the ongoing discussions and progress being made regarding transfer tools such as model clauses (Council of Europe, Association of South East Asian Nations (ASEAN), the Ibero-American Data Protection Network (RIPD)) and certification (Global Cross-Border Privacy Rules (CBPR) Forum and the European Data Protection Board (EDPB).

To further advance these efforts, the DPAs encourage dialogue between organisations and networks to develop convergent transfer mechanisms. In this context and as outlined in this year’s Action Plan,5 the DPAs themselves endeavour to share knowledge on tools for secure and trustworthy transfers, notably through the comparison of CBPR and EU certification requirements.5

The G7 DPAs also welcomed the reference to DPAs as stakeholders in the future “Institutional Arrangement for Partnership” (IAP), a new structure the G7 Digital Ministers announced in their 30 April 2023 Declaration6 to operationalise DFFT. The IAP means to bring together stakeholders and the broader multidisciplinary community of data governance experts to advance DFFT, with DPAs being the only example of experts addressed explicitly7. In this forum, DPAs must have a key role in contributing on topics that are within their competence and unique expertise in order to ensure that high standards of data protection
and privacy will be upheld. The G7 DPAs are therefore closely monitoring the development of IAP and are committed to help shape it in a manner that keeps data protection and privacy at its core.

**Promoting Privacy in Emerging Technologies**

Another topic high on the agenda of G7 DPAs are technological developments that need to be regulated in ways that reinforce trust and respect privacy. While emerging technologies such as AI, the Internet of Things (IoT) and cloud services may bring substantial benefits to global economies, societies and the personal lives of their users, the DPAs point out that these technologies can also cause serious harm and undermine individual rights and interests if left unchecked.

The G7 DPA Roundtable draws particular attention to privacy enhancing technologies (PETs) that can help controllers and processors implement data protection principles and safeguards into their processing activities effectively. PETs however are not the sole solution when it comes to data protection and privacy concerns and should not be seen as a “silver bullet.” Controllers and processors will still have to assess how and to what extent individual PETs can enhance compliance with data protection requirements on a case-by-case basis. The group understands that usage of PETs requires guidance by DPAs and has agreed to develop a joint terminology document outlining key terms and characteristics regarding de-identification, anonymisation, pseudonymisation and other PETs to ensure a common understanding, but also highlight important differences between jurisdictions. In addition, the DPAs are developing a use case demonstrating how the use of a specific PET (synthetic data) can reduce privacy risks. The case study aims at bringing regulatory insights to this emerging market and in doing so, encourage the responsible use of such new technologies.

**Generative AI on the rise**

Besides PETs, one of the main issues on the mind of G7 DPAs tech experts continues to be AI. AI technologies have been at the core of the Roundtable’s discussions since the very beginning and gained even more relevance in recent months due to the increase of generative AI applications. Such technologies however do not exist in a regulatory void and ensuring the trust of individuals, regulatory authorities and society as a whole is essential to their expansion and continued use. In their 2023 Communiqué, the G7 DPAs therefore stress that developers and users of these technologies need to demonstrate compliance with existing legal obligations and ensure the implementation of risk mitigating measures – which might require consultation with DPAs, where necessary and appropriate.

Given the rapid evolution of generative AI and its increasing use, the G7 DPAs also decided to adopt a separate Statement on Generative AI outlining the group’s position towards opportunities and challenges arising from generative AI technologies. One of the document’s underlying key messages is that AI is by no means a law-free zone: current law applies to generative AI products and uses, even as different jurisdictions continue to develop new AI-specific laws and policies.

To inform future development and deployment of generative AI, the G7 DPAs laid down some main areas of concern. These include the lack of legal authority for the processing of personal information during all stages of development and use of generative AI – for the datasets used to train, validate and test generative AI models, for processing personal data resulting from individuals’ interactions with generative AI tools and for the content generated by these tools. Besides, generative AI tools need to adhere to fundamental principles of data protection and privacy, such as data quality, transparency, data minimisation, purpose limitation, data subject rights, documentation and accountability. Developers and providers need to keep these principles in mind and should also implement security safeguards against possible threats and attacks (e.g. attacks that might seek to invert the generative AI model to reproduce personal information that was processed to train the datasets or to subvert the efficacy of data protection measures in other ways).

**Global Enforcement**

However, high data protection and privacy standards are futile if they cannot be enforced. The G7 DPAs reaffirmed the need for international cooperation among DPAs in order to effectively exercise their regulatory powers, especially in the face of new and emerging technologies and increasing global data flows. To facilitate effective enforcement in practice, the group declared that they would increase communication on regulatory measures and share domestic and international best practices both within the G7 and with other regulatory authorities.

The DPAs highlight the work of existing fora and instruments for cooperation, such as the GPA’s International Enforcement Working Group (IEWG) and Global Cross-Border Enforcement Cooperation Arrangement (“Mauritius Arrangement”)10, the Global Privacy Enforcement Network (GPEN), the European Data Protection Board’s (EDPB) toolbox on essential data protection safeguards for enforcement cooperation11 and the Global Cooperation Arrangement for Privacy Enforcement (CAPE)12.

**The Future of the G7 DPA Roundtable**

The G7 DPAs are committed to strengthen cooperation and address the challenges identified in the 2023 Action Plan to work towards a high level of data protection and privacy on a global level. The Roundtable has consequently been established as a permanent and important forum in the G7 DPAs’ schedules with annual meetings at commissioner level and continued exchange at expert level; it has also been endorsed by the G7 Digital Ministers in their annual Declarations since 202113.

The 2023 Action Plan foresees further tangible results and output that put the G7 DPAs policies into practice. The group aims to develop these topics and projects under the 2024 chairpersonship of the Italian DPA (the Garante) and will evaluate its progress and achievements at the next G7 DPA Roundtable meeting in Italy.

**Author**

Marc Schlegel is a Legal Officer at Germany’s Federal Commissioner for Data Protection and Freedom of Information, Division 14 - European and International Affairs. Email: Marc.Schlegel@bfdi.bund.de
Revised Swiss DP Act now in force

The law, inspired by the GDPR and revised to maintain a free flow of data between the EU and Switzerland, entered into force on 1 September.

New elements include Data Protection Impact Assessments for the processing of sensitive data, records of processing activities (ROPA), Data Protection Advisors (DPOs) and data breach reporting. Privacy by Design is also now explicitly mentioned.

The revised law applies to the processing of personal data of natural persons. The previous law also included legal entities.

The Data Protection Commissioner will start charging private sector companies fees for some of his services, for example opinions on codes of conduct and data protection impact assessments, and approval of Standard Contractual Clauses and Binding Corporate Rules. The processing of complaints remains free of charge.

- See the new Data Protection Act at www.coeib.admin.ch/coeib/en/home/datenschutz/grundlagen/ndsg.html

How is AI being implemented and used globally?

An international research project seeks to measure progress, with the aim of issuing benchmarks to assist governments’ decision-making. By Laura Linkomies.

The attempt to deliver a global index on responsible AI will serve as a measurement tool for countries that are in different stages of maturity, Dr Rachel Adams, Principal Researcher, ICT Africa explained at The Institute of Advanced Legal Studies event on 6 September. Outlining the project, she said that a pilot is currently being concluded in the study that draws from experience in 140 countries.

Adams said that existing work on ethics and AI at the OECD or UNESCO is valuable, but are they globally inclusive? The OECD obviously not, but generally speaking, too often AI development is based largely on Western thinking and values. Adams sits on numerous boards and expert panels including the UNESCO Expert Group on the Implementation of the UNESCO Recommendation on AI in Ethics, and the expert advisory board of an Ada Lovelace project on the future of AI and genomics, and is therefore well informed.

“Generative AI has raised new issues. What matters is that these systems are based and trained on data of Western populations, but then taken to the global South,” Adams said. “AI is contributing to global inequality. One of our research questions is whether responsible AI is a globally relevant concept.”

Some of the first extensive consultations have taken place in Francophone Africa, for example in women’s groups and other under-represented groups.

“We found out that we must address the full AI lifecycle. Human rights must extend behind political rights to include social and economic rights. The responsibility of the private sector must be addressed.” In many economies, the question is not just about laws and frameworks, but also access to computers and broadband, she said.

Objectives of the project
The Global Index on Responsible AI, a project of Research ICT Africa and the Data for Development Network (D4D.net), is funded by the government of Canada. The Global Index has established an international research network as well as a core project team that operates under the guidance of an Expert Advisory Committee (EAC), which in turn is composed of global experts on the responsible use of AI.

The project will develop inclusive, measurable indicators that reflect a shared understanding of what responsible AI means in practice, and track the implementation of responsible AI principles by governments and key stakeholders.

The aim is to provide comprehensive, reliable, independent, and comparative benchmarks for governments so that they can assess progress of responsible AI and its implementation compared with the rest of the world.

During the seminar, there was a discussion on whether we should also be measuring forms of irresponsible AI and how it is being used. It was thought that despite spooky examples of where AI can go very wrong (Chat GPT used in court to deliver a verdict, and similar), there should be more advantages than disadvantages – as long as we are clearer how to deploy the technology.

Methodology
The programme webpage describes the work: “The methodology of the Global Index focuses on the development of core indicators and the collection of primary data relating to country-level commitments and progress on responsible AI. This work is supported by an extensive secondary data review and analysis. Regional research hubs have been established to oversee country-based researchers around the world and ensure the quality of the data collected.”

Independent researchers have been recruited at country-level to gather primary data. Governments are asked to complete a questionnaire on work in progress.

The 140+ national researchers are selected, trained and supervised by the Regional Hubs, which will be responsible for the quality of the collected evidence and its assessment.

Benchmarking and DP aspects
The evidence-based benchmarking will enable government and community leaders to develop and strengthen national initiatives, fostering responsible AI use and monitoring progress over time.

Adams explained how benchmarking would work; for example a binding instrument in a country would score more highly than a non-binding one. The researchers are now waiting for data to come in from the pilot studies to decide on how to calculate the scores.

Adams said that the project touches on many data protection variables, for example bias. This concept has been defined in some 1,000 words, but different countries can take a different interpretation – the project allows for cultural divergence. For example, the definition of what is ethical varies hugely in different parts of the world.

Project timeline
The first edition of the Global index on responsible AI will be available in early 2024. After that, countries can start using the Index in 2024 – 2025. This will involve working with regional hubs, Chief Sales Officers, and governments to engage with the index and report findings.

Information
Dr Rachel Adams is Principal Researcher at ICT Africa and the AI4D African Observatory on Responsible AI. Adams is also an Associate Fellow of the Leverhulme Centre for the Future of Intelligence at the University of Cambridge, and a Research Associate of the Information Law and Policy Centre at the Institute of Advanced Legal Studies, University of London.

See ilias.sas.ac.uk/events/lpc-ai-humanities-seminar-series-toward-a-global-index-measuring-state-responsible-ai and www.responsibleaiindex.org
México has not yet explicitly included biometric data as a special category of personal data (or sensitive data), but this has not stopped the national Data Protection Authority from deciding that this data will be protected as such. How is it doing it so?

If you ask GDPR professionals about how biometric data is regulated in the European Union (EU) it is pretty sure all of them will tell you that “biometric data for the purpose of uniquely identifying a natural person” is deemed as a special category of personal data (namely “sensitive data”). This is also the case in some Latin American countries, where biometric data is explicitly protected as a sensitive data.

WHAT DOES THE LAW SAY IN MEXICO?


The Data Protection Laws do not provide definitions of “biometric data” but do include definitions of what “sensitive data” means. “Sensitive data” definitions use a mixed approach to explain sensitive data:

- the definitions provide that sensitive data INCLUDE this type of information: personal data that may reveal aspects such as racial or ethnic origin, present and future state of health, genetic information, religious, philosophical and moral beliefs, trade union affiliation, political opinions and sexual preference.
- the same “definition” provides that sensitive data include such personal data that affect the most intimate sphere of a data subject, or whose improper use may give rise to discrimination or entails a serious risk for data subject.

Thus, this definition includes three criteria (the “Sensitivity Criteria”) that may be used (or misused) to conclude that certain personal data shall be deemed as “sensitive”:

1. If a personal data affects the most intimate sphere of a data subject, it shall be deemed as sensitive, or
2. If the improper use of a personal data may give rise to discrimination, it shall be deemed as sensitive, or
3. If the improper use of a personal data entails a serious risk for the data subject, it shall be deemed as sensitive.

Under these criteria, it can be argued that a last name or a postal code shall be deemed as sensitive data if a given controller may use them to exclude individuals from a recruitment procedure or governmental benefits procedures when data subjects have certain last names or live in certain postal zones.

However, we shall also consider that “discrimination” does not only refer to the most common (and negative) meaning of such action, but also includes “the ability to see the difference between two things or people” and that every selection exercise is basically a discrimination process.

What does it mean or what constitutes “the most intimate sphere” of an individual? Does it mean the same for you and me? Does it mean the same in different countries? The Data Protection Laws (as you may guess) does not provide a definition or an explanation of such concept.

Finally, we want to note that the notion of “serious risk” is also tricky, given that processing personal data comes with an implicit risk that under certain circumstances it shall be deemed as low, medium, or high. When is it then an “improper” use of a personal data that entails a serious risk for the data subject?

INAI ISSUED GUIDANCE IN 2018

With this legal definition at hand, in 2018 Mexico’s Data Protection Authority (known as the INAI) issued the ‘Guidelines for the Processing of Biometric Data’ where, using European sources like the Working Party 29’s ‘Opinion 3/2012 on developments in biometric technologies and the GDPR’, established a reference document to explain biometric data, but remained unclear on specific situations where biometrics data shall also be deemed as sensitive.

The most significant advance comes from a series of examples where Mexico’s Data Protection Authority states that: “For example, the biometric data of the iris could be considered sensitive in those cases in which it allows obtaining information about the data subject’s health status. Likewise, a fingerprint could be considered sensitive if, through its improper use, it could provide access to privileged information that could jeopardize the security or stability of the data subject’s assets.”

In this scenario, and however difficult to explain and apply the Sensitivity Criteria might be, they are jointly used by the Mexican Data Protection Authority to define in several sanctioning procedures that every biometric data is sensitive data, even when it is not used for the purpose of uniquely identifying a natural person (e.g. when using biometric technology for authentication purposes). This has led to several fines when data controllers did not correctly categorize the type of data they were processing and for this reason they did not obtain the relevant and mandatory consent to process sensitive data - in Mexico, an explicit and written consent.

HOW CAN ORGANISATIONS PREPARE?

In practice, Mexican data controllers and processors have started to understand (some the hard way) that processing biometric data is a serious matter,
1. Under the guidance of the INAI, "private parties" current legal framework applicable to private data controllers under the law by treating this data as sensitive data. Assessments are not (yet) mandatory for private data controllers under the current legal framework applicable to “private parties”.

In the end, two things are certain: 1. Under the guidance of the INAI, biometric data is and will be protected as sensitive data, following European standards, and 2. An update of the Data Protection Laws is necessary in order to clarify the scope of protection of certain data and to establish as mandatory specific measures to carry out DPIAs.

After all, Mexico is a non-European signatory country of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and we shall honour our obligations.

---

### Ireland’s DPA fines TikTok €345 million for unfair processing of children’s data

Following the European Data Protection Board’s binding dispute resolution decision, Ireland’s Data Protection Commission (DPC) announced on 15 September its final decision which requires TikTok to bring its processing into compliance in the EU by taking the action specified within a period of three months; and pay administrative fines totalling €345 million.

The decision relates to child users of TikTok, and the company’s infringement of the GDPR’s fairness principle. It was found that TikTok failed to provide sufficient transparency information to child users, and that it implemented ‘dark patterns’. There were also issues regarding platform settings for child users.

“While there was broad consensus on the DPC’s proposed findings, objections to the draft decision were raised by the Supervisory Authorities of Italy and Berlin (acting on behalf of itself and the Baden-Württemberg SA),” Ireland’s DPC said.

Anu Talus, EDPB Chair, said: “Social media companies have a responsibility to avoid presenting choices to users, especially children, in an unfair manner – particularly if that presentation can nudge people into making decisions that violate their privacy interests. Options related to privacy should be provided in an objective and neutral way, avoiding any kind of deceptive or manipulative language or design. With this decision, the EDPB once again makes it clear that digital players have to be extra careful and take all necessary measures to safeguard children’s data protection rights.”

The decision relates to the processing of data of registered TikTok platform users, who are aged between 13 and 17 years old, in connection to certain design practices, as well as certain issues relating to age verification and other issues regarding children under the age of 13.

TikTok, which has its EU headquarters in Ireland, says that most of the criticisms are no longer relevant as a result of the changes it has introduced.

---

### European Commission designates Gatekeepers under the Digital Markets Act

On 6 September, the European Commission designated six companies as gatekeepers under Article 3 of the Digital Markets Act (DMA). The new designation applies to Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. They now have six months to submit a detailed compliance report to outline how they will comply with each of the obligations of the DMA. For example, companies are no longer allowed to track end users outside of the gatekeepers’ core platform service for the purpose of targeted advertising, without effective consent.

In case a gatekeeper does not comply with the obligations laid down by the DMA, the Commission can impose fines up to 10% of the company’s total worldwide turnover, which can go up to 20% in case of repeated infringement.

The Commission has opened four market investigations to further assess Microsoft’s and Apple’s submissions arguing that, despite meeting the thresholds, some of their core platform services do not qualify as gateways:

- **Microsoft:** Bing, Edge and Microsoft Advertising
- **Apple:** iMessage.

---

© 2023 PRIVACY LAWS & BUSINESS

PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT  OCTOBER 2023  27
Join the Privacy Laws & Business community

The PL&B International Report, published six times a year, is the world’s longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B’s International Report will help you to:

- Stay informed of data protection legislative developments in 180+ countries.
- Find out about future regulatory plans.
- Learn from others’ experience through case studies and analysis.
- Understand laws, regulations, court and administrative decisions and what they will mean to you.
- Incorporate compliance solutions into your business strategy.
- Be alert to future privacy and data protection law issues that will affect your organisation’s compliance and reputation.

Included in your subscription:

1. Six issues published annually
2. Online search by keyword
   Search for the most relevant content from all PL&B publications.
3. Electronic Version
   We will email you the PDF edition which you can also access in online format via the PL&B website.
4. Paper version also available
   Postal charges apply outside the UK.
5. News Updates
   Additional email updates keep you regularly informed of the latest developments.
6. Back Issues
   Access all PL&B International Report back issues.
7. Events Documentation
   Access events documentation such as PL&B Annual International Conferences, in July, Cambridge.
8. Helpline Enquiry Service
   Contact the PL&B team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.
9. Free place at a PL&B event
   A free place at a PL&B organised event when booked at least 7 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

PL&B Reports are an invaluable resource to anyone working in the data privacy, e-commerce or digital marketing fields. Unlike many news feeds or updater services, each Report provides rare depth of commentary and insight into the latest developments.

Rafi Azim-Khan, Partner, IP/IT & Head Data Privacy, Europe, Pillsbury Winthrop Shaw Pittman LLP


Stay informed of legislative developments, learn from others’ experience through case studies and analysis, and incorporate compliance solutions into your business.

UK Report

Subscriptions

Subscription licences are available:
- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the Report in any way, the unexpired portion of your subscription will be repaid.