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 uncertaind 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 on 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;

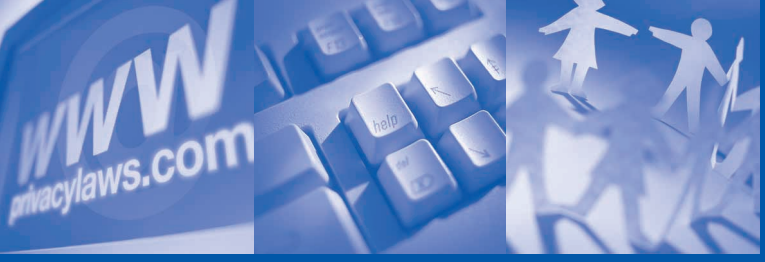
- the transfer results in the provision of a service or benefit for the data subject; or
- the transfer is to conduct scientific research and studies.

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.

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



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

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*[1] was passed by both houses with no debate, and no requirement of committee consideration. It received Presidential assent on 11 August

Continued on p.3

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.

Continued on p.9

Issue 185 **OCTOBER 2023**

INTERNATIONAL report

ISSUE NO 185 OCTOBER 2023

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Professor Graham Greenleaf
UNSW, Australia

Ceyhun Necati Pehlivan
Linklaters, Spain

Brian Meenagh and Lucy Tucker
Latham & Watkins, Saudi Arabia and UAE

Marc Schlegel
Office of Germany's Federal DPA

Héctor E. Guzmán Rodríguez
BGBG Abogados, Mexico

Tom Cooper
PL&B Deputy Editor

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

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 is 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.

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.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

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.

privacylaws.com/reports

> *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**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the current Data Protection and Digital Information Bill, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

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

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.