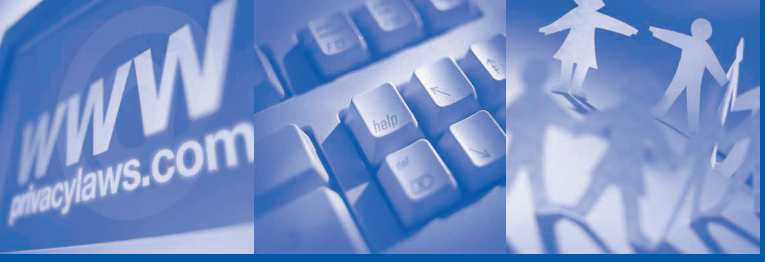

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

How consistently is the EU GDPR being enforced?

The European Union's data rules have built-in consistency mechanisms. After five years of operation, how well are they working and what does the future hold? **Tom Cooper** reports.

The uniform application of the EU's General Data Protection Regulation (GDPR) across the bloc's 27 Member States, each with a different history, legal system and attitude to data protection, was always going to be a challenge. Nevertheless, that is the European Data Protection Board's (EDPB's) remit under EU law.

In May, the board elected Finland's Data Protection Commissioner, *Anu Talus*, as its new chair[1].

Continued on p.3

Texas enacts comprehensive privacy law

Jorge Ortiz, **Nicholas Shepherd**, and **Lindsey Tonsager** of Covington & Burling analyse the law which enters into force in July 2024.

On 18 June 2023, the Governor of Texas signed into law the Texas Data Privacy and Security Act (TDPSA), making it the 12th state overall in the United States, and seventh in 2023 alone, to enact a comprehensive privacy law.[1]

With approximately 30 million inhabitants, Texas is the second-most populous state (behind only California) to pass a privacy law of this scope and magnitude. The TDPSA

Continued on p.4

Issue 184 **AUGUST 2023**

INTERNATIONAL report

ISSUE NO 184 **AUGUST 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
Jorge Ortiz, Nicholas Shepherd, and Lindsey Tonsager
Covington & Burling LLP, US
Pablo Palazzi,
Allende & Brea, Argentina
Peter McLaughlin and Ashfin Islam
Armstrong Teasdale LLP, US
Nana Botchorichvili
IDEA Avocats, France
Juliette Faivre
University of Cambridge, UK
Asher Dresner
Freelance writer, UK
Tobias Lunn
University of Nottingham, UK
Gabrielle Hornshaw
University of Nottingham, UK

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

Future prospects for the EU-US privacy framework

Organisations have been pleased to see the adoption of the new EU-US Privacy Framework in July (p.7). It is almost certain that a legal challenge will arise – nevertheless companies now have some breathing space provided that companies sign up to the pact enthusiastically and implement their commitments in the US.

The next step is the EU Commission's long-awaited review of the existing adequacy decisions. Argentina, which is one of the beneficiaries, is now modernising its law to meet the higher GDPR-level of adequacy (p.17). The bill is based on the EU GDPR and the Council of Europe Convention 108+.

On the back of the EU-US decision, we can expect a UK decision soon, as well as Switzerland taking similar measures. But what about adequacy at US state level? The trend of adopting state level consumer privacy laws continues with Texas (p.1) and Oregon (p.6). There have already been speculations about California being a likely candidate for adequacy as it has a stronger law than the other states. Also possible are sectoral arrangements which would benefit the areas currently not covered by the Privacy Framework, such as financial services.

The Cambridge Analytica saga continues, as witnessed by our expert panel at *PL&B's* summer conference (p.14). In Australia, the Privacy Commissioner and Meta have now been ordered by the federal court to engage in mediation. This is to end the costly legal proceedings over the scandal which started five years ago.

Some worrying developments can been seen in the adoption of generative AI (p.28). The EU is not just paying attention but is at the forefront with its AI Act, and evaluating the impact of AI in the metaverse from many viewpoints (p.6). On the positive side, SupTech which includes AI elements can help DPAs with their workload (p.18).

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.

Texas.. from p.1

will take effect on 1 July 2024, giving companies that fall within its scope approximately a year to ensure their data collection practices comply with the law.

The TDPSA is comparable in certain respects to Virginia's Consumer Data Protection Act (VCDPA) and other state privacy laws following a similar model, but deviates in certain key areas, as noted below. More generally, the TDPSA and other state privacy laws significantly align with the blueprint of the European Union's General Data Protection Regulation (GDPR), a model which continues to proliferate worldwide.

This article provides an overview of key aspects of the TDPSA, considers where the law falls compared to other comprehensive state privacy laws enacted in the US to date, and raises practical considerations for covered businesses to bear in mind.

Applicability and scope

The TDPSA applies to any natural or legal person that meets the following (cumulative) criteria:

1. conducts business in the State of Texas or produces products or services consumed by Texas residents;
2. processes or engages in the sale of personal data; and
3. is not a small business as defined by the United States Small Business Administration, with some exceptions.

This scope deviates from other state privacy laws that define specific volume thresholds of personal data that an organization must collect/process in order for the law to apply.[2]

That said, the TDPSA contains many of the same explicit exceptions from its scope as other state privacy laws. For example, the TDPSA does not apply to state agencies, higher education institutions, nonprofit organizations, or entities subject to federal laws such as the Health Information Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA). Moreover, the TDPSA does not restrict a controller's ability to, for example, comply with the law, nor to prevent, detect, or respond to security incidents. Similar to other state privacy laws thus far (except for California), the law's provisions do not extend to individuals acting in the employment or commercial context.

Key definitions

The TDPSA includes definitions that align with common terminology used in other state privacy laws and the GDPR, such as "personal data" (any information that is linked or reasonably linkable to an identified or identifiable individual), "controller" (a party that, alone or jointly, determines the purpose and means of processing personal data), and "processor" (a party that processes personal data on behalf of a controller).

Notably, the TDPSA (similar to the state privacy laws in Colorado and Connecticut) includes a definition of "dark pattern" that refers to a user interface designed with the effect of substantially subverting or impairing user autonomy, and includes any practice the Federal Trade Commission refers to as a "dark pattern." The TDPSA also includes definitions for the terms "sale" (a disclosure of personal data to a third party for monetary or other valuable consideration), "profiling," and "sensitive data" that align with other state privacy laws' definitions.

Controller obligations

Parties operating as data controllers subject to the TDPSA must comply with a range of obligations and restrictions. Below, we have identified six key obligations that controllers operating in Texas should bear in mind, and considered some of their practical implications.

1. Transparency: Controllers must provide consumers with a reasonably

accessible privacy notice that specifies:

1. the categories of personal data processed by the controller;
2. the purpose for processing personal data;
3. if applicable, the categories of personal data the controller shares with third parties;
4. if applicable, the categories of third parties with whom the controller discloses personal data; and
5. how consumers may exercise their rights and a description of the methods for a consumer to submit a request to exercise their rights.

Many companies operating in Texas may have already drafted and published such notices to comply with the GDPR or other privacy laws and/or align with industry practice more generally, but would be well-advised to review them again from the perspective of their data collection practices in Texas, to ensure these notice requirements are adequately addressed.

2. Data Minimization: Controllers must limit data collection to what is reasonably necessary in relation to the purpose(s) for which the personal data is processed, as disclosed to the consumer. This may require organizations to (if they have not done so already) identify the specific personal data elements they are collecting, make a clear connection between those elements and the purpose(s) for which they are used, and plainly disclose this information in the privacy notice. Notably, companies subject to the TDPSA will have to obtain opt-in consent to process any personal data that is not reasonably necessary to fulfill a processing purpose disclosed in the privacy notice.

3. Consent to Process (and Notice to Sell) Sensitive Data: Controllers must obtain consent before processing a consumer's sensitive data. "Sensitive data" is defined as personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, sexuality, or citizenship or immigration status; genetic or biometric data processed to identify individuals; personal data collected from a known child; and precise geolocation data (i.e., identifies a consumer within a radius of 1,750 feet, 533 metres). If a controller sells sensitive data or biometric data, it must post a specific notice (i.e. "NOTICE: We may sell your [sensitive/biometric] personal data.") in its privacy notice.

4. Controller-to-Processor Contractual Terms: Similar to the GDPR and other state privacy laws, the TDPSA requires that specific contractual terms be included in agreements between controllers and processors in relation to the processing of personal data, including, for example, provisions requiring the controller to provide clear instructions for the processing and for the processor to, in turn, maintain the confidentiality and security of the data, cooperate with reasonable requests of the controller in relation to the data, return or delete the data at the conclusion of the services (unless prolonged retention is required by law), and so forth.

5. Data Protection Assessments: The TDPSA requires controllers to conduct data protection assessments of processing activities that involve targeted advertising, the sale of personal data, profiling (in limited circumstances), sensitive data, or otherwise present a heightened risk of harm to consumers. The assessments must identify and weigh the benefits of the processing to the controller, consumer, other stakeholders, and the public at large, against the potential risks to the consumer, while also taking into consideration any mitigating safeguards to reduce risks.

Consumer rights

The TDPSA affords consumers the following rights:

- Confirm whether a controller is processing their personal data and access to such personal data;
- Correct any inaccuracies in the personal data;
- Delete personal data;
- Obtain a portable copy of the consumer's personal data that allows the consumer to readily transmit the data to another controller; and
- Opt-out of processing for purposes of (a) targeted advertising, (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

The TDPSA also requires controllers to implement opt-out preference signals by 1 January 2025. Specifically, a consumer may designate an authorized agent using a technology, including a "global setting on an electronic device," that allows the consumer to opt out of the processing of personal data for targeted advertising, the sale of personal data, or both. A controller must comply with an opt-out preference signal if the controller is able to verify the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

Enforcement and guidance

The Texas Attorney General has the exclusive authority to enforce the TDPSA, and can seek injunctive relief or civil penalties of up to $7,500 per violation. The TDPSA provides controllers and processors with a 30-day "cure period" to remedy a violation. This cure period will remain in effect indefinitely, unlike some other state privacy laws recently enacted, which include a cure period that will expire on a certain date.

Separately, the TDPSA requires the Attorney General to post on its website information relating to: (1) the responsibilities of a controller; (2) the responsibilities of a processor; and (3) facilitating consumer rights. Moreover, the Attorney General must provide and maintain an online channel through which consumers may submit complaints.

High-level comparison to other state privacy laws

The California Consumer Privacy Act of 2018 (CCPA) was the first comprehensive state privacy law enacted in the US, and none of the state privacy laws promulgated since then have aligned closely to the CCPA approach – which, among other things, uses unique terminology (e.g., "business" and "service provider" instead of "controller" and "processor"), creates a state-level privacy authority, and establishes a limited private right of action. Instead, the other state laws thus far align with the more general framework of the GDPR, and the six laws enacted in 2023 mirror the approach of the laws in place in Virginia, Colorado, Connecticut, and Utah (the first four states to introduce privacy laws following the CCPA).

Overall, the TDPSA tracks most

closely with Virginia's VCDPA. However, the TDPSA has a distinct way of addressing the opt-out preference signal, as described above.

Practical considerations for businesses

As a starting point, any business operating in Texas or targeting Texas consumers should consider whether the TDPSA applies to it. As previously mentioned, the TDPSA uses unique applicability criteria, such that it is possible that a business operating across multiple states that is not subject to the VCDPA or other state privacy laws could fall within the scope of the TDPSA. It would also be prudent to monitor any official statements clarifying the TDPSA's scope of application, such as the Attorney General's forthcoming guidance.

Lastly, if a business has determined that the TDPSA applies to it, it should be able to at least partly leverage its US state privacy compliance efforts to address TDPSA obligations. Depending on the business, there may also be some TDPSA-specific considerations that should be reviewed to ensure full compliance, like the specific privacy notice requirements for controllers that sell sensitive or biometric data.

AUTHORS

Jorge Ortiz and Nicholas Shepherd are Associates, and Lindsey Tonsager is a Partner at Covington & Burling LLP.
Emails: jortiz@cov.com
nshepherd@cov.com
ltonsager@cov.com

REFERENCES

1 Tex. H.B. 4, 88th Leg., R.S. (2023). Other states with comprehensive privacy laws include California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Montana, Florida and Oregon.
2 For example, the VCDPA applies to a person that conducts business in Virginia or produces products or services that are targeted to Virginia residents and that (1) controls or processes personal data of at least 100,000 consumers; or (2) controls or processes personal data of at least 25,000 consumers and derives over 50 percent of gross revenue from the sale of personal data.

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 and events. You can then click straight through from the search results into the PDF documents.

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 in Data Protection and related laws.

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.

privacylaws.com/reports

"*PL&B UK and International Reports* are valuable and trusted resources for our office, offering timely, in-depth analyses about emerging issues in the world of global data protection. This publication is *de rigueur* for anyone who works in the fast-paced and constantly evolving privacy field."

Michael McEvoy, Information and Privacy Commissioner for British Columbia, Canada

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.