HERZOG

HERZOG FOX & NEEMAN

The Delaware Personal Data Privacy Act

Herzog's Compliance Playbook

October 2025

HERZOG
HERZOG FOX & NEEMAN

The Delaware Personal Data Privacy Act

INTRODUCTION

Delaware's Personal Data Privacy Act, which came into force in the beginning of 2025, establishes new obligations for businesses processing personal data, emphasizing **transparency**, **accountability** and **responsible data management**. Covered businesses must enable individuals to **access**, **correct** and **delete** their personal data, and provide **clear mechanisms to opt out** of certain processing activities. The new act further requires businesses to maintain transparent data practices, restrict data use to disclosed purposes and implement **structured compliance measures** to safeguard consumer privacy.

Many **businesses that are incorporated in Delaware for corporate or other legal reasons may still fall within the act's scope**, as the thresholds are relatively low compared to other privacy regimes. Therefore, it is essential to assess carefully whether your business is subject to the act. Businesses should note that **the right to cure violations ends on 31 December 2025**, meaning that after this date, enforcement actions by the Attorney General can proceed immediately without the opportunity to cure violations to avoid the enforcement action.

This Playbook is designed to help determine whether the law applies to you, what your key obligations are, and how to prepare for compliance.

KEY MILESTONES

1 January 2025

The main obligations in the act came into effect. Covered businesses (controllers) must:

- Provide clear and accessible privacy notices to consumers;
- Respond to consumer rights requests;
- Implement data minimization practices and safeguards for sensitive data;
- Ensure contracts with service providers include required provisions under the act;
- Maintain records and internal compliance processes.

1 January 2026

- Violations of the act can be enforced immediately without the opportunity to cure;
- Recognition of Universal Opt-Out Signals becomes effective.
  From this date, covered businesses must honor standardized privacy signals (e.g., Global Privacy Control) automatically, allowing consumers to exercise their opt-out rights more easily.

WHO IS A COVERED BUSINESS?

Under the act, a covered business, bound by the rules, is any entity that meets the following criteria:

a. **Either conducts business in Delaware OR targets Delaware residents** - "Conducting Business" under the act may include any of the following activities:

   i. Operating physical or online stores, services or platforms accessible to Delaware residents;

   ii. Offering goods or services to Delaware residents, even if the entity is not physically located in Delaware;

   iii. Marketing or advertising products or services directly to Delaware residents;

   iv. Engaging in other commercial activities reasonably directed toward Delaware residents.

   AND

b. **Met <u>one</u> of the thresholds in the act in the previous calendar year:**

   i. Controlled or processed personal data for 35,000 or more Delaware consumers, **or**

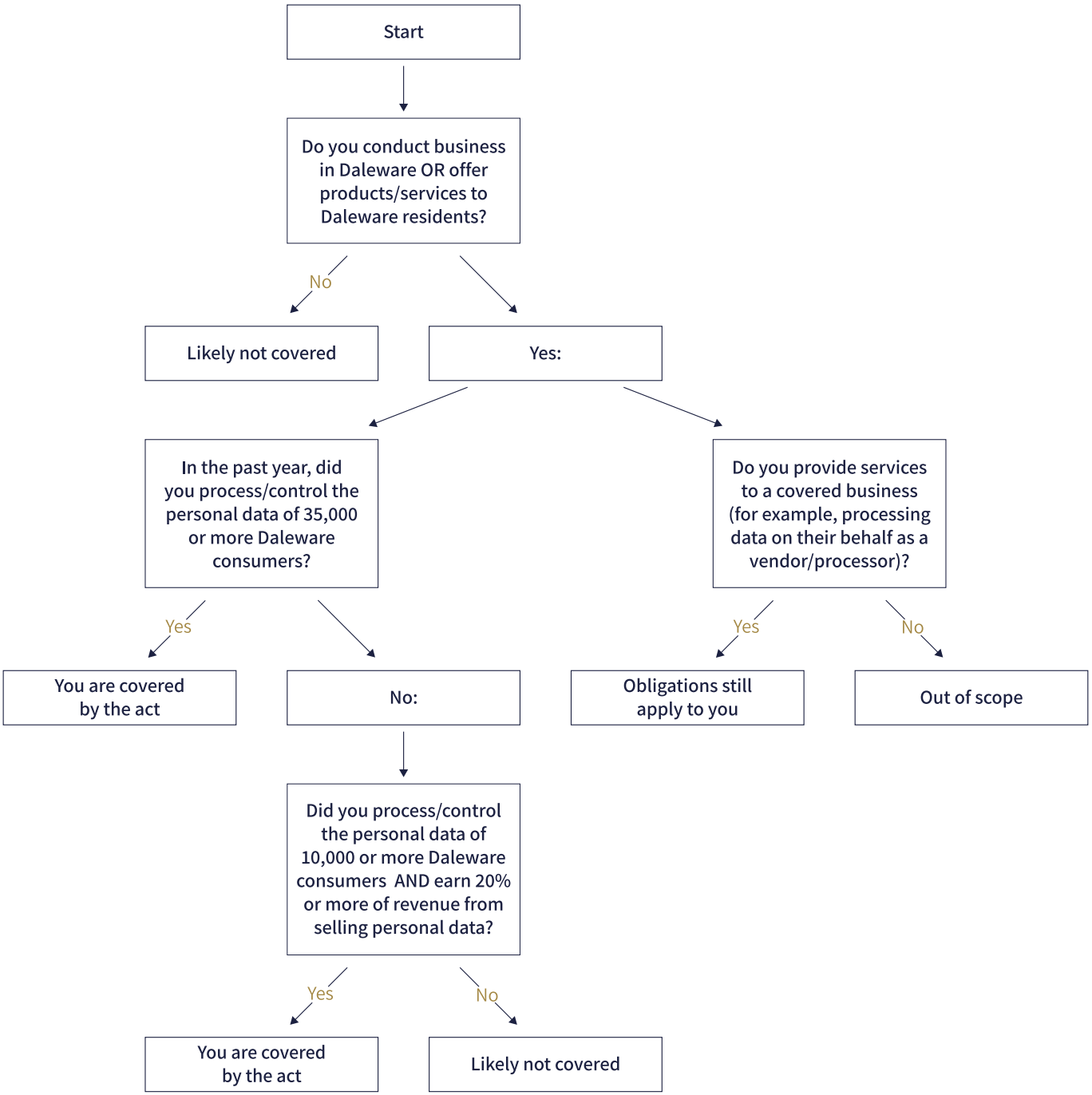
   ii. Controlled or processed personal data for 10,000 or more Delaware consumers **and** derives more than 20% of its gross revenue from the sale of personal data.

Service providers processing data solely on behalf of another business are **generally not directly covered**, unless they independently determine the purposes and means of processing personal data. However, various obligations pursuant to the act would be indirectly imposed on them by the relevant covered business.

HERZOG
HERZOG FOX & NEEMAN

The Delaware Personal Data Privacy Act

ARE YOU A COVERED BUSINESS?



KEY OBLIGATIONS AND COMPLIANCE STEPS

The act establishes core obligations for covered businesses, emphasizing transparency, consumer control and accountability. Compliance involves both legal and operational measures.

Privacy notices and transparency

Businesses must provide **clear, accessible and comprehensive privacy notices** explaining what personal data is collected, why it is collected, how it will be used, with whom it is shared and whether it is sold or used for targeted advertising. Notices must also **describe how consumers can exercise their rights**.

TO DO Review and update all privacy notices to meet the act's disclosure standards.

Consumer rights

Data subjects (consumers) are entitled to access, correct, delete and obtain a copy of their personal data, as well as opt out of the sale or use of their personal data for targeted advertising.

TO DO Implement a reliable process to receive, authenticate and respond to consumer requests within 45 days (extendable once if reasonably necessary).

TO DO Maintain logs of all consumer requests and responses.

TO DO Implement technical measures to enable submitting an opt-out request using Universal Opt-Out Signals.

Data minimization and sensitive data

The act requires that personal data collected be **limited to what is reasonably necessary for stated purposes.** Processing **sensitive data** (such as health, biometric, or children's data) requires prior **opt-in consent.**

TO DO Conduct a data mapping exercise to identify sensitive data categories, and ensure appropriate consent mechanisms are in place.

Information security

Covered businesses must implement and maintain reasonable technical, administrative and physical **safeguards** proportional to the sensitivity and risk associated with personal data processing.

TO DO Develop or enhance information security policies, perform risk assessments, and apply additional controls for high-risk processing activities.

KEY OBLIGATIONS AND COMPLIANCE STEPS

The act establishes core obligations for covered businesses, emphasizing transparency, consumer control and accountability. Compliance involves both legal and operational measures.

Service provider management

Contracts with service providers that handle personal data must include provisions on confidentiality, data return or deletion upon termination, compliance with the act and assistance with fulfilling consumer rights requests.

TO DO Review and update all vendor agreements to ensure they meet statutory requirements and document all service provider relationships.

Record keeping and internal governance

Covered businesses should maintain **internal records** of personal data processing activities, consumer requests and compliance actions. Regular reviews should be conducted to ensure policies remain aligned with legal requirements.

TO DO Schedule periodic privacy audits and document compliance measures.

Policy updates and ongoing compliance

Compliance is an **ongoing obligation** that requires continuous monitoring and adjustment of privacy practices.

TO DO Conduct a comprehensive gap analysis to evaluate your current privacy policies, internal processes and technical controls against the acts requirements, identifying any areas that fall short of compliance. This should be based on a data mapping exercise to understand what personal data your business collects, from whom it is obtained, how it is used and with whom it is shared. The results of these assessments can be used to update your internal governance framework, employee procedures and public-facing privacy notices.

TO DO Implement an internal policy ensuring continuous monitoring of your data processing activities and regulatory developments, as well as periodic updating of the related procedures and policies.

OUTRO

Delaware's new data privacy act applies to businesses that meet the definition of a covered business, which includes entities collecting personal data of Delaware residents, conducting business in or targeting Delaware residents, and meeting certain thresholds.

Compliance requires transparency, consumer rights management, data minimization, security, proper service provider agreements and internal governance.

Businesses should be aware that **the right to cure for violations ends on 31 December 2025**, after which enforcement by the Attorney General may occur immediately. By establishing a structured, risk-based privacy compliance program, your organization can meet the act's requirements and strengthen overall consumer trust.

If you're unsure whether your organization falls under this law or need assistance developing compliant privacy notices and opt-out mechanisms, our team can guide you through the process and help you prepare for upcoming milestones, including the effective recognition of **Universal Opt-Out Signals by 1 January 2026.**

HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions, digital platforms** and leading **self-regulatory guidelines**. This enables our team to offer **practical, holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

Regulation of **personal information** has been dramatically expanding on a global basis. Companies processing data of hundreds of millions of data subjects as well as small start-ups - all are required to spend significant resources on understanding and implementing the constantly evolving legal challenges. Our Privacy & Data Protection team guides our clients on all matters relating to their data usage and assist them in navigating the numerous data protection regimes, in all the jurisdictions in which they operate.

HERZOG
HERZOG FOX & NEEMAN

The Delaware Personal Data Privacy Act

Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il

Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il

Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il

Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il

Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il

Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il

Or Noy | Associate
Technology Regulation
noyo@herzoglaw.co.il

On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il

Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il

Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il

Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il

Yonatan Glatt | Associate
Technology Regulation
glatty@herzoglaw.co.il

Benjamin (Ben) Reznik | Associate
Technology Regulation
reznikb@herzoglaw.co.il

Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il

Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il

Kobi Plotkin | Associate
Technology Regulation
plotkiny@herzoglaw.co.il

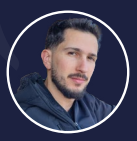
Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il

Yuval Glazer | Associate
Technology Regulation
glezery@herzoglaw.co.il

Yoel Toledano | Intern
Technology Regulation
toledanoyo@herzoglaw.co.il

Elias Shehadeh | Intern
Technology Regulation
shehadehe@herzoglaw.co.il

Gal Mechtinger | Intern
Technology Regulation
mechtingerg@herzoglaw.co.il



Elad Rozenvasser | Intern
Technology Regulation
rozenvassere@herzoglaw.co.il