DATA PROTECTION ASSESSMENTS: A NEW ARSENAL FOR COMBATING CYBERATTACKS

by Lynn Rohland

In a landscape where the average cost of a data breach reached an all-time high of $4.88 million in 2024 — a 10% increase over the previous year — data protection assessments (DPAs) serve as a preemptive tool to identify vulnerabilities in the data processing value chain, such as weak encryption or third-party sharing risks. They also enable companies to implement targeted safeguards, such as multi-factor authentication or regular vulnerability scans. Here, you will find key insights into why, by whom, when, and where DPAs are necessary, as well as best practices for completing them.

Link Between Cybersecurity and DPAs

As Texas is one of the largest and most economically thriving states, it's no surprise that it is also a central hub for digital commerce and activity. With countless organizations and individuals relying on digital systems to drive business models and conduct daily affairs, robust data protection laws are justified. This is where the Texas Data Privacy and Security Act (TDPSA) steps in.

CYBERSECURITY AWARENESS MONTH

Amid the dynamic framework of data protection laws, the TDPSA, effective as of July 1, 2024, strongly emphasizes completing DPAs as a cornerstone for safeguarding the personal information of consumers, prospective customers, and clients (also known as data subjects). Why? Performing DPAs offers substantial benefits to businesses, particularly in bolstering defenses against escalating cybersecurity threats. They also align distinctively with the TDPSA's cybersecurity mandates, which require controllers to establish and maintain reasonable administrative, technical, and physical data security practices proportionate to the volume and nature of personal data processed. That means transforming DPAs from a mere 'checkbox' compliance activity into a strategic asset for risk reduction.

TDPSA At-A-Glance

The TDPSA is packed with mandates universally applicable to a company or individual that meets any of the criteria stated in the law 88(R) HB 4:

1. conducts business in Texas or produces a product or service consumed by residents of Texas;
2. processes or engages in the sale of personal data (this includes maintaining personal information of consumers, clients, and business partners); and
3. is not a small business, as defined by the United States Small Business Administration (SBA), except where Section 541.107 applies to a person as described by the subdivision.

The regulation's privacy and cybersecurity requirements are designed to safeguard the confidentiality, integrity, and availability of personal data and sensitive information in both online and offline environments.

CYBERSECURITY AWARENESS MONTH

It establishes expectations and provides a framework for how organizations collect, store, access, process, and share personal data. In short, it serves as a countermeasure against the increasing threats of data breaches, identity theft, and other cybercrimes.

Designated Assessors

The TDPSA specifies who — in particular, controllers that are entities that determine the purpose and means of processing personal data — is required to conduct and document DPAs for high-risk activities. Activities include:

- targeted advertising,
- the sale of personal data,
- profiling that may have legal or significant effects, and
- the processing of sensitive data such as racial or ethnic origin, health information, or biometric data

These assessments must identify and weigh the direct and indirect benefits of the process. They evaluate benefits (or potential harm) to the controller, consumers, stakeholders, and the public against specific risks to consumer rights and incorporate IT controls and security measures to mitigate risks.

CYBERSECURITY AWARENESS MONTH

Assessment Catalysts

Controllers are required to conduct and document DPAs for certain "processing" activities — an operation or set of operations performed manually or automatically on data, including the collection, use, storage, disclosure, analysis, deletion, or modification of personal data. When they are required includes:

1. the processing for targeted advertising,
2. the sale of personal data,
3. the processing for purposes of profiling,
4. the processing of any sensitive data; and
5. any processing activities that might present a heightened risk of harm to consumers.

High-Risk Deep-Dive

DPAs are designed to evaluate high-risk scenarios, emphasizing a balanced assessment that considers consumer expectations, the context of processing, and the use of de-identified data to reduce risks. The prerequisites exist to embed "privacy by design" principles into organizational practices. This compels businesses to anticipate and mitigate threats like unauthorized access or data breaches before they occur, protecting consumers from identity theft, discrimination, or other harms.

Several areas in the value chain where a process would necessitate a DPA include one or more of the following:

- processing involves the use of innovative technologies,

- any decision made about an individual's access to a product, service, opportunity, or benefit is based to any extent on automated decision-making or involves the processing of sensitive personal data.
- any profiling of individuals on a large scale,
- any processing of biometric data,
- any processing of genetic data other than that processed by a general practitioner or health professional for the provision of health care is directly provided to the individual,
- combining, comparing, or matching personal data obtained from multiple sources,
- processing of personal data that has not been obtained directly from the individual in circumstances where the controller considers that compliance would prove impossible or involve disproportionate effort,
- processing, which involves tracking an individual's geo-location or behavior, including but not limited to the online environment,
- the use of the personal data of children or other vulnerable individuals for marketing purposes, or to offer online services directly to children, or
- the action of processing data is such that if a data breach occurred, it could jeopardize the [physical] health or safety of individuals.

Combating Cyberattacks

By mandating DPAs for handling personal and sensitive data, the TDPSA helps ensure businesses evaluate potential cyberattack vectors, such as phishing or ransomware. This leads to enhanced incident response plans that can reduce breach containment time by up to 9 days compared to unprepared organizations.

CYBERSECURITY AWARENESS MONTH

The result? Organizations with robust risk assessment processes, including DPAs, experienced 61% lower breach costs, saving an average of $2.66 million per incident. In Texas, where the law's business-friendly approach allows DPAs to leverage existing assessments from laws such as the European Union's General Data Protection Regulation (GDPR) Data Protection Impact Assessment (DPIA), companies can streamline compliance while fostering a culture of cybersecurity awareness. This turns potential liabilities into competitive advantages by building consumer trust and minimizing the financial fallout from attacks that affected more than 3,158 U.S. entities in 2024.

In 2024-2025 trends, businesses conducting regular DPAs reported a 24% decrease in ransomware incidents, as these assessments uncover gaps in data flows that hackers exploit, aligning with broader U.S. trends where states like Colorado and Virginia mandate similar evaluations to preempt harms. For Texas businesses, avoiding civil penalties of up to $7,500 per violation – 1,000 records equating to potentially up to $7.5M in fines – and achieving cost savings through faster breach detection. Organizations with mature assessment programs identified breaches an average of 64 days quicker. The value of a collapsed timeline cannot be overstated.

As cyber disruptions escalate, the healthcare industry alone experienced 725 breaches exposing 133 million records in 2023. DPAs under the TDPSA serve as an arsenal for innovation, enabling secure AI-driven processing or cross-border data transfers while safeguarding against 46% of breaches stemming from stolen credentials. These assessments elevate cybersecurity from a reactive stance to a proactive strategy, ensuring sustained compliance and protecting stakeholders in an increasingly hostile digital environment.

CYBERSECURITY AWARENESS MONTH

Leading Practices

The why of conducting DPAs is to evaluate the potential for significant physical, material, or non-material harm to individuals. DPAs should obtain a clear understanding of a specific processing activity and its potential impact on data subjects (e.g., consumers, customers, and business partners) about whom personal data is being processed, the possible impact on other processing activities, risk to the IT systems, programs and enterprise levels, and risk to complying with an organization's privacy principles, internal policies, and applicable privacy laws and regulations.

Gray Reed Advisory Services begins by identifying (and weighing) the direct or indirect benefits processing agreements to the controller, the consumer, or to other stakeholders. Specifically, we evaluate the benefits against potential risks to the rights of the individual associated with that processing activity, which should include a risk mitigation strategy of safeguards and technical measures the controller can deploy to reduce such risks.

There are multiple approaches an organization can take to define, organize, and document a DPA Template to perform assessments. Gray Reed Advisory Services DPA Template guidance is three-fold:

1. Think more broadly: When creating the DPA template, don't take too narrow an approach, as you may inadvertently exclude critical details during an opportunity to glean pertinent information that may have a direct, indirect, or tangential impact on the process assessed or information depended upon by other organizational goals, initiatives, and future business needs. For that reason, ensure your DPA template captures the appropriate insights needed while avoiding the trap of over-engineering.

2. Socialize the template: Often, organizations distribute templates or questionnaires for assessments and audits without confirming a user's understanding of the template, the questions posed, and how to respond to them, creating additional legwork or misunderstandings. Organizations should consider performing a 'pilot test' of their DPA template on a select group of users or hold an online seminar to step through an illustrative example, including user "Do's and Don'ts" to solicit feedback and update the template and its instructions accordingly.
3. Stakeholder Reviews: If a member from the organization's Office of Privacy is completing the DPA, an excellent leading practice is to send the stakeholder the questions to be asked or the answers to be validated in advance of a meeting. Demystifying meeting topics and questions ahead of time greatly increases stakeholder participation, the information's accuracy, and the timely completion of DPAs. Once a DPA is completed, consider reverting to the primary contributor(s) – especially if the business process is more complicated – for a final review.

Final Thoughts

Beyond Texas and the EU, several U.S. states have adopted similar mandates. For instance, Colorado, Connecticut, Virginia, Oregon, and Indiana require data protection assessments for high-risk processing. New 2025 laws in Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, and Maryland incorporate assessment obligations as well. These state laws, often modeled after comprehensive frameworks like California's CPRA, aim to harmonize privacy protections amid a patchwork of regulations, ensuring businesses proactively address vulnerabilities in an era where data breaches surged by 70% in 2024, exposing billions of records.

CYBERSECURITY AWARENESS MONTH

DPAs are indispensable in the fight against cyber threats, offering businesses under the TDPSA and similar laws a structured path to security and compliance. By embedding risk evaluation into core operations, DPAs mitigate the human and financial toll of breaches, which continue to escalate despite technological advances. With more states mandating these assessments, proactive adoption will distinguish resilient organizations from vulnerable ones, safeguarding the digital economy.

Contact Us

Lynn Rohland
Gray Reed Advisory Principal
703.801.6075 | lrohland@grayreedadvisory.com

Vicky Fang
Gray Reed Advisory President
408.203.8778 | vfang@grayreedadvisory.com