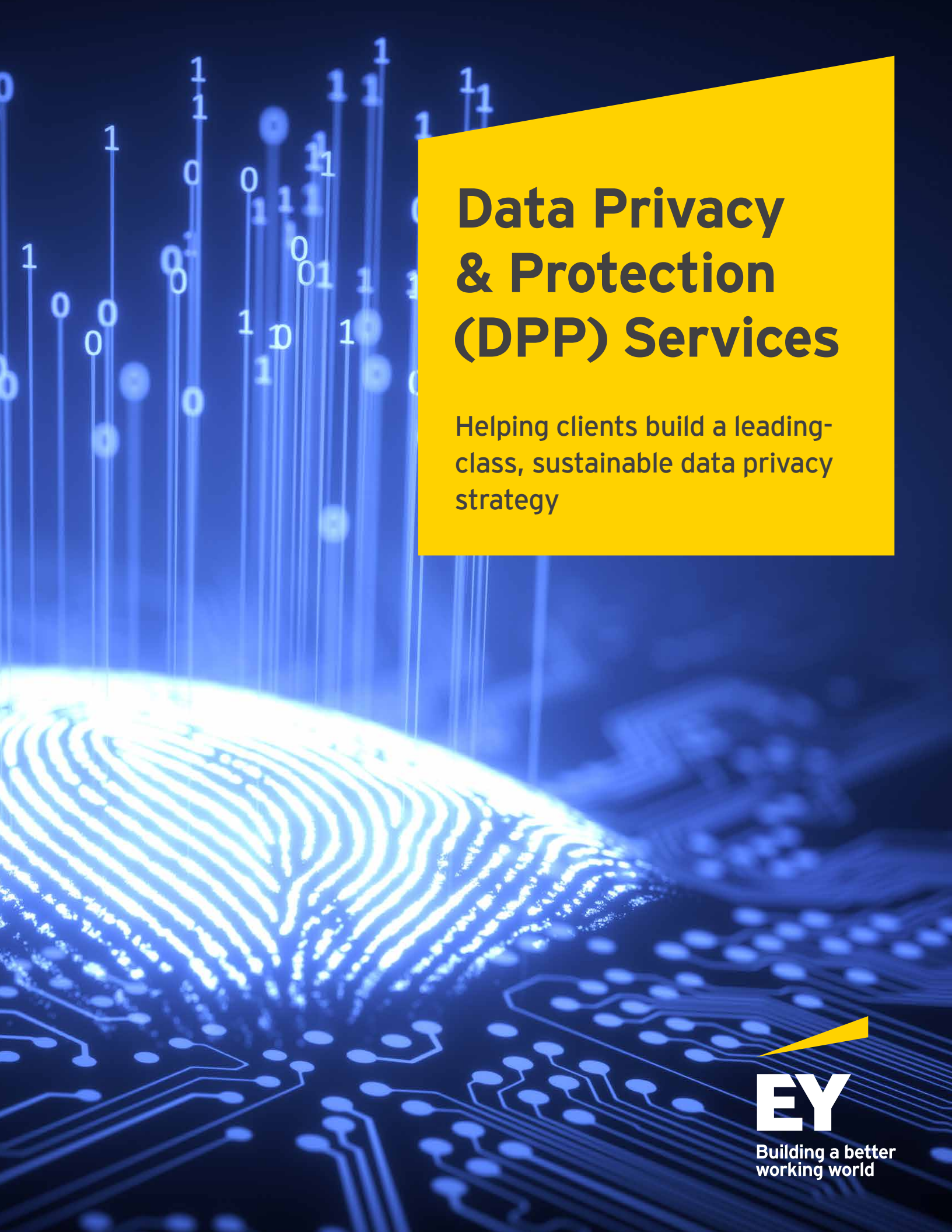
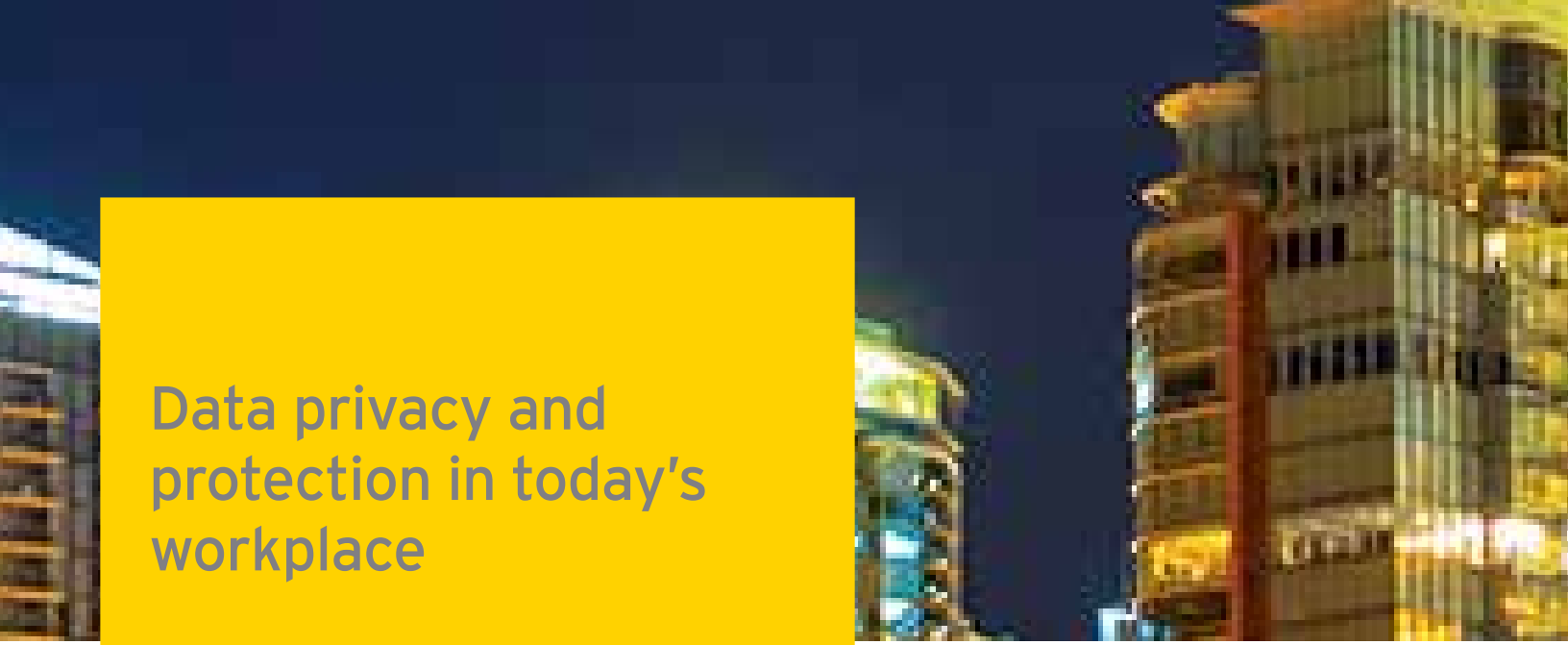


Data Privacy & Protection (DPP) Services

Helping clients build a leading-class, sustainable data privacy strategy

EY
Building a better working world



Data privacy and protection in today's workplace

Changing legislative requirements, most recently demonstrated by the European Union's General Data Protection Regulation (GDPR), Personal Information Protection and Electronics Document Act (PIPEDA) and California Law, coupled with increasing customer expectations, pose a rising number of challenges for companies.

In framing privacy, most companies adopt a compliance-centric view. While this may be crucial in light of the wealth of regulatory requirements, it frequently overshadows the opportunities that are to be found in advancing your company's data privacy and protection profile. Data privacy and protection can not only give you a competitive advantage, but in the age of increasing consumer awareness and digital interconnectivity, transparency is key to achieving and maintaining the trust of your clients. And a properly executed data privacy and protection strategy can achieve just that.

At EY, we're focused on helping companies build a leading-class, sustainable data data privacy and protection strategy that incorporates customer rights and ethical use of data that adheres to legal and compliance obligations.

Why should your organization care about Data Privacy & Protection (DPP)?

In the digital age, it's very easy to leak confidential information or fall victim to an online breach. Here are some shortcomings we have seen at other organizations when data privacy and protection are not properly managed:

- Oversharing/processing of personal information
- Unable to effectively respond to data subject requests or data breach
- Unable to demonstrate accountability and compliance
- Good intention but misuse of data
- Third-party service provider weakness
- Electronic media loss
- Website leakage
- Unwarranted marketing communications
- Fraudulent transactions
- Social engineering, including phishing

These situations can have serious implications for your organization from both the internal and public perspectives. If not handled properly, mismanaged data could result in...

- Identity theft, either by a customer or employee
- A hit to your company's brand and reputation
- Direct financial loss
- A loss of consumer and business partner confidence
- A loss of market value
- Litigation or regulatory action
- Becoming the industry example of what could go wrong

Fortunately these issues can be resolved before they reach catastrophic levels. At EY, we can help your organization build a sustaining data privacy and protection program to implement the proper protection measures, while also helping to transform your business to efficiently comply with the latest regulations. A sustainable DPP program is built around three main pillars: Governance, Use of Data and Validation. EY offers a wide range of DPP services in the three pillars to help organizations build sustainable DPP programs.

Why EY?

The global EY network comprises over 500 dedicated DPP consultants in more than 30 countries. Our DPP advisors can address companies' global needs and requirements in different fields including Legal because the EY DPP practice is also supported by EY Law, the Firm's Legal arm that can respond to our clients concerns on DPP legal implications all over the world. A significant number of our DPP professionals are active members of the International Association of Privacy Professionals (IAPP) and more than 200 are Certified Information Privacy Professionals (CIPP) for Canada (/C), Europe (/E), US Government (/G), US private sector (/US) or Asia (/A), Certified Information Privacy Technologists (CIPT), or Certified Information Privacy Managers (CIPM). As part of our relationship with the IAPP, on a yearly basis, EY supports the global preparation and distribution of the Privacy Governance Report where multiple trends are analyzed to help the DPP community make decisions supported by thoughtful insights.

Our DPP advisors are also connected to other professional associations relevant for the privacy community like ISACA, $(ISC)^2$, ACFE and IIA with the intention of offering an holistic approach when helping organizations respond to their DPP related challenges.

We draw on our global network to deliver insights into legislation and regulations across the world. For over a decade, EY has helped international organizations understand DPP risks and compliance, as well as regulations, thereby helping them effectively manage the use of personal information in their organizations.

EY uses a risk-based, multi-disciplinary approach supported by robust tools and methodologies to help clients understand the impact of DPP on their organization, achieve timely and consistent DPP compliance and leverage DPP for wider strategic benefit. EY has identified key software vendors in the market that support the definition of a DPP management and accountability program and has developed business relationships with them to be ready to serve clients that might be interested in the use of these tools.

With deep industry and client knowledge, EY has helped clients achieve both compliance and competitive advantage through effective DPP programmes, from gap analysis to ongoing managed services.

Is your company ready to transform?

Privacy program transformation

Using a four-stage approach – understand, assess, define and implement – we integrate privacy-related components into your company's daily processes. Not only can this approach act as a driver for keeping up with the changing privacy regulatory landscape, but it can also help raise your organization's overall data maturity. By doing this, you can extend your existing capabilities of data usage and increase the effectiveness of current data analytics and dashboarding activities.

DPP is not a compliance issue – it's strategic!

How we will work with you:

Every business is unique and requires a different approach to DPP. We offer a variety of services to effectively cater to your organization's goals. We'll work alongside you to support, train and implement effective procedures within your business, to help you comply with the latest regulations and also think about the future.

A sustaining DPP program is built around three main pillars: Governance, Use of Data and Validation. EY offers a wide range of DPP services in the three pillars to help organizations build sustainable DPP programs.

Governance

DPP workshop

Our workshop can help your organization understand that DPP is more than solely a compliance or security issue. An overview of the changing regulatory landscape will form the starting point of the workshop, followed by a highly interactive three-hour session. During the session, we'll approach DPP from multiple angles to help you better navigate this complex landscape and truly understand its impact on your organization. Through the workshop, we'll link DPP to business initiatives such as digital transformation and analytics. By delivering the interactive breakout sessions, our DPP advisors will share leading practices and lessons learned.

Assessment and roadmap

Often combined with the DPP workshop, our team executes our readily available DPP assessments to determine gaps between your organization's current and desired state. This provides input for the roadmap towards DPP regulations compliance.

During this assessment, we check important themes, such as current data processing roles, responsibilities, data leakage procedures, data flows and data usage. We compare the results to common market practices as well as legal obligations. This allows for determining the impact of new topics, such as the right to be forgotten and explicit consent, on current operations. We subsequently drive development on a practical roadmap which clearly states goals and purposes to foster organizational acceptance.

Privacy by design implementation

Privacy by design and by default is a crucial requirement for an effective DPP strategy. It allows you to promote privacy and data protection from the design phase and embed privacy considerations throughout the lifecycle of a project.

We can help you develop a privacy by design methodology that you can effectively incorporate in your current development and design of systems, processes and products. We can also assess the current process and systems to determine which are at risk from a privacy perspective and determine what considerations should be implemented.

Data flow mapping

The mapping of data flows can enhance the successful implementation of DPP. The identified data streams can be used to respond to the compliance requirements (based on applicable laws and regulations) and to set up data protection.

Current data mapping activities are often executed with an IT mindset, thereby creating results that are too detailed for business application and become outdated as soon as they're created. The focus is often placed on specific technical fields, rather than the types of data used by business processes. Our service is designed to enforce the appropriate focus which, combined with the application of data discovery tooling and a strong data governance structure, can significantly raise the effectiveness of the exercise.

Privacy impact assessments (PIA)

The ability to consistently perform high-quality PIAs throughout the organization is gaining in importance with a view towards regulatory compliance. PIAs are required in Canada and are of critical importance for the GDPR as Data Protection Impact Assessments. A PIA is a useful tool to embed DPP into the design of all processes and applications that process personal data.

We can support the design and execution of PIAs, while making use of our designated tool set. Additionally, we can provide training to your teams to raise organizational awareness and execution power.

Data Breach Notification & Incident Management

Recent changes to regulations are putting stricter requirements on organizations to ensure they have effective data breach notification and incident management procedures that include effective recording, resolving and reporting processes.

EY's services include creating a data breach notification and incident management program that includes processes around how incidents and breaches are reported and assessed for severity, a protocol for severity classification, required actions, roles and responsibilities, escalation paths based on the type or severity training, and root cause analysis.

Privacy Management and Accountability Program

A DPP program needs to be managed in a way that responds to corporate needs and, to be successful needs to be adopted by the entire organization through accountability. Different executives within the organization need to be aware of the responsibilities they have to support the privacy program and have to be held accountable on the compliance supporting actions.

Our methodology can help on defining a holistic privacy management program that covers the organization end to end while identifies the executives that need to be held accountable and helps define tools and processes to verify that accountability over time.

Our services at various stages in the data privacy and protection journey:

Find out which service is right for your business.

Use of Data

Anonymization and pseudonymization to enable data analytics

We can help you make great use of the data your organization collects while simultaneously enabling privacy compliance. By analyzing each step in the data analytics process, it can be determined if it's necessary to make data anonymous, or if you should apply pseudonyms to data tags. Given the flexibility of current data tools, existing data is easily combined with new sources, which could result in unforeseen identification possibilities.

Our service can help you prevent any misplaced data enrichment without downsizing the power of data analytics.

Identity & Access Management (IAM)

Implementing DPP starts with giving access to any private data that's available in the organization only to authorized people. This results in a tight linkage of specific roles and access levels and the business processes in which they act.

Continuous access management is becoming one of the foundational cornerstones of organizational DPP enablement. Our IAM portfolio contains a suite of complementary services that operationalize policies, processes and supporting technologies that enable an organization to manage access to its resources over time. Our services are focused on business enablement and help an organization to identify opportunities to continuously and efficiently manage system access and mitigate risks to confidentiality, integrity and availability of critical data. We understand how relevant IAM is for defining an effective DPP model, however, an organization does not only need to protect personal data and complying with DPP regulations needs to be linked to the corporate compliance requirements in order to respond to the related compliance risks in the most efficient way. Our experience on DPP and cybersecurity allows us to be able to have a holistic view on defining an IAM program that not only responds to DPP compliance requirements but to broader organizational needs.

Cross-Board Data Management

Transferring personal data across jurisdictions requires understanding the different regulations to respond to, for example, the GDPR allows data transfers to countries that provide an "adequate" level of personal data protection as determined by the EU. Transfers may also be allowed to non-EU states without an adequate level of personal data protection, provided they use other protection methods such as the use of standard contractual clauses or binding corporate rules.

Our services include establish mechanisms, such as binding corporate rules/Intra Group Agreement [internal]; EU Model Clauses [external]) to monitor the internal and external transfers of data outside of the European Economic Area. We can align these mechanisms with the supervising authority, formalize a procedure, appoint an accountable person for managing the transfer of data and establish a process/procedure or tools to help move data appropriately across borders.

Data Retention & Records Management

Data retention is a significant activity within an overall data lifecycle management framework. Data should be retained for at least a minimum duration that's governed by applicable laws, regulations, subject area, and local policies and guidelines.

As part of our services, we develop an overall structure – processes, routines, time frames and system support – for deletion, anonymization or pseudonymization of personal data based on statutory retention periods and internal policies. Where possible, we indicate where the data retention should be mitigated through automation in the IT systems.

Data Leakage Prevention (DLP) and Incident Response

Understanding data flows will help an organization comprehend where data is allocated when in rest and when in motion. In any stage of the flow, data can face risk situations.

We can help you identify those risks and define efficient controls to respond to them. These controls can be supported by processes or tools that will prevent, detect or correct events where data leakages happen.

Our services at various stages in the data privacy and protection journey:

Find out which service is right for your business.

Validation

DPP managed services

Our portfolio of managed services has been specifically designed to meet the unique requirements of any organization in a flexible and customized way. Depending on factors such as organizational setup, maturity and resourcing, we can offer a different managed service – or combination of services – to meet your specific objectives.

For example, an organization might want to outsource repeatable tasks by using services such as a managed privacy impact assessment (PIA). Or it may be looking for guidance to support monitoring activities, using managed data privacy analytics.

Whatever your concerns and priorities around GDPR compliance, we have a managed service that can meet them.

Third Party & Vendor Management

Our vendor management services include due diligence processes to cover third-party activities related to information security, procurement, contracts, DPP and independence. We use industry-standard security assessments to evaluate inherent and residual risk across DPP and cyber security, compliance and other third-party risk categories such as data classification, data location, and access and data transmission.

Security & Privacy SOC2 Reports

SOC 2 examinations are designed to deal with an organization's controls relevant to the systems it uses to process users' data. The resulting report helps users of the data understand the effectiveness of the organization's controls and how they integrate with controls at the user entity.

Our team examines and reports on system controls set forth in the AICPA's trust services criteria.

Table Top Exercises

With the rising tide of DPP incidents and the systemic impact they can have on financial systems, organizations have recognized the need to enhance regular business continuity and crisis management planning with specific cyber incident simulations.

EY's table top exercises related to data loss includes planning, designing and developing a table-top DPP incident simulation exercise for your crisis response team which mimics the impact of a significant attack. We can facilitate immersive exercises with your teams, bringing high levels of engagement and a sense of realism through the use of visual aids, social media injects and other collateral factors.

Contact us

For more information, please contact one of our professionals below.

Yogen Appalraju
Canadian Cybersecurity Leader

yogen.appalraju@ca.ey.com
+1 416 943 5902

Carlos Perez Chalico
Senior Manager, Data Privacy & Protection

carlos.perez.chalico@ca.ey.com
+1 416 943 5338

Nicola Vizioli
Associate Partner, Data Privacy & Protection

nicola.vizioli@ca.ey.com
+1 514 879 8046

David Witkowski
Manager, Employment and Data Privacy & Protection Law

david.witkowski@ca.ey.com
+1 416 932 5841

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

For more information about our organization, please visit ey.com/ca.

284010
ED 00

ey.com/ca