Introduction

Data privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information.

Changing regulatory requirements – including GDPR – are combining with rising customer expectations to create growing challenges around data privacy.

However, companies that take a compliance-centric approach to data privacy are missing out on an opportunity to gain competitive edge.

EY’s data privacy service offering helps clients blend data privacy with transparency - equipping them to win customers’ trust and loyalty in a GDPR world.
Demonstrating data privacy for GDPR and beyond

In May 2018, the EU’s new GDPR ushered in unprecedented levels of data protection for EU residents, backed by fines of up to €20 million or 4% of global revenue, whichever is higher.

Although GDPR brings a welcome harmonization of fragmented data protection laws across EU Member States, its wide-reaching impact and stringent rules require a fundamental organizational shift, even for businesses compliant with existing legislation. When the steep financial penalties for non-compliance and data losses are added to the cost of reputational damage, sanctions, remediation and the potential impact on digital transformation, the risk of inaction is clear.

GDPR Impact

GDPR is a transformational effort that touches on all aspects of an organization, reaching across people, processes and technology.

Process

- Organizations will need to determine which business and IT processes are impacted by GDPR requirements.
- GDPR will require organizations to redesign their processes to incorporate steps that address key privacy requirements.
- Organizations must implement process monitoring controls to provide transparency that the processes consistently satisfy GDPR requirements and are updated as necessary.

People

- Organizations will need to identify the relevant stakeholders across business units, including HR, who can contribute to compliance remediation planning and execution.
- The GDPR will require organizations to adequately train employees responsible for handling EU data with their obligations for supporting GDPR compliance.

Technology

- Organizations must understand their IT environment, data assets, and data processing applications to identify the impacts that GDPR requirements present and to develop a remediation plan to update the IT environment to support GDPR compliance.
- Organizations should consider various tools available for automating GDPR compliance operations to an enterprise scale.
GDPR challenges and how EY can help

Apart from the urgency of working towards compliance there is also the opportunity to take a strategic approach to GDPR. EY’s risk-based, multi-disciplinary approach targets GDPR investment where it matters most for regulatory compliance and competitive advantage. Drawing on our extensive privacy knowledge and proven tools and methodologies, we help to identify clients’ highest risks, and design and execute a tailored road map for compliance and beyond.

When it comes to demonstrating clients compliance with the GDPR, EY’s data privacy assurance services give clients independent assistance about their data protection controls. The benefits of data privacy assurance include:

- Indicating compliance to supervisors and other external stakeholders
- Showing that organizations have implemented Processes and controls to protect personal data
- Demonstrating that organizations execute procedures to limit the possibility of a data breach

The three services that support achieving these benefits are:

- GDPR Independent Review Services
- Attestation Report based on International Standards on Assurance Engagements (ISAE) 3000
- GDPR Certification

Although these are not mutually exclusive, deciding which service an organization requires depends partly on which GDPR category it falls into (see graphic).

What does your organization need?

Organizations that want to demonstrate their compliance with the GDPR first need to ensure that they meet its requirements. In practice, many organizations are finding this a challenging goal and some have a significant distance to go. EY offers a range of services - including a detailed attestation program, leading to a future GDPR certification.

![Diagram showing the services and decision points for GDPR compliance.]

Organization wants to demonstrate GDPR compliance

- Report is for internal purpose only (Assurance pre and post implementation)
  - Compliance, DPO Function, Processes and Control Review only
    - GDPR Independent Review

- Report is for external purpose and seek certification
  - EY Attestation and Certification path
    - EY Attestation Service:
      - Set Up Attestation procedures
      - ISAE 3000 Attestation report
  - EY Certification
    - GDPR Certificate

Organization should request this type of service:
Your challenge

Your business has an internal need either to obtain a diagnostic before GDPR transformation project or demonstrate the quality of its implemented privacy processes and controls.

How EY can help

EY can provide the business with GDPR Independent Review Services, which comprise assurance services customized and tailored to your business needs. Being either focused on specific or full scope privacy processes and controls (or your DPO function), it aims to demonstrate that the business’s processing activities have been audited. Reports being provided are addressed to management and other authorized internal stakeholders to either prepare implementation project or obtain post-implementation assurance. Once GDPR compliance is reached, attestation and certification are typically straightforward process.

Your challenge

Your business has an external need to demonstrate or disclose the implementation of privacy processes and the operating effectiveness of the controls in these processes.

How EY can help

EY can audit the design and operating effectiveness of the privacy processes and the operating effectiveness of the controls in these processes to help the business to obtain GDPR Attestation and GDPR Certification, both based on the CARPA scheme as issued by CNPD, the Luxembourg national data protection regulator.

EY can help throughout your business GDPR journey to certification with the following services:

- **EY Attestation Report**: CNPD CARPA mechanism provides a set of criteria to comply with before being certified. This enables the audit activities to be performed based on regulator’s criteria on the organization’s implemented privacy controls and to conclude on these controls effectiveness. This will result in ISAE 3000 report being issued, leading to GDPR Certification.

- **GDPR Certification**: EY will seek to become accredited by CNPD to act as GDPR Certification Body. EY will then make a formal communication to CNPD in the role of an authorized body and propose a formal GDPR certificate to be issued by CNPD. To reach this state, EY, as a certification body, will review the conformity and the scope of your privacy processes and controls based on the ISAE 3000 GDPR Attestation Report.
Navigating the GDPR challenges

To help our clients, EY has developed DPO One - an integrated platform consisting of tools and services.

How EY’s DPO One Platform can support your entire organization in operationalizing the GDPR?

Our value proposition
Why our clients should use DPO One

1. Management in Control
   DPO One enables to show that the C-suite and DPO is in the control of the GDPR-related activities.

2. Reduce risk & regulatory exposure
   DPO One supports the client identifying and reducing privacy risks within their practice. As such, it enables them to reduce regulatory exposure and helps meeting the different GDPR requirements.

3. Avoidance of costs
   Having a clear picture of the GDPR compliance activities and knowing where the high risks sit, can lead to avoidance of costs such as fines (e.g., 4% of global annual revenue), audit costs and other expenditures.

4. Constant multidisciplinary support
   DPO One enables the client to have the constant support of a global organization as EY on their activities and challenges related to GDPR. The operating model allows multidisciplinary support from Advisory, Regulatory, FIDS,...

5. End-to-end
   DPO One is one of the most complete GDPR-specific solutions in the market, covering all the requirements of the regulation.

6. Integrated and integrable solution
   All the modules (and related services) of the solution are integrated, ensuring consistency. The solution itself is integrable with the client’s environment.

7. Scalability and up-to-date
   DPO One is scalable, both from a platform and service point of view. The client can start small, and acquire new modules and services only when required. Updates provided both from a platform and content perspective (e.g., regulatory updates).

8. Recognized industry practice
   DPO One leverages the recognized industry practices developed by EY at a global level, allowing clients to increase their maturity posture in an efficient manner.

DPO One is based on four building blocks:

1. Dashboarding: DPO One comes with a dashboard, providing your organization with a single overview of the GDPR compliance activities based on the selected modules.
2. Modules: DPO One consists of several technical modules to operationalize the various aspects of GDPR.
3. Intelligence: DPO One facilitates the identification and maintenance of the regulatory requirements to keep the selected modules up-to-date.
4. DPO One Support: The DPO One offering is not just a platform and tooling, but also involves our multidisciplinary DPO support team, adding human intelligence to the platform.
### Benefits of the DPO One Solution

<table>
<thead>
<tr>
<th>Ready to go</th>
<th>Industry practice</th>
<th>Platform</th>
<th>Pick and choose</th>
<th>Cloud-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>The platform is ready for deployment</td>
<td>Services are based on EY's recognized industry practices and experiences</td>
<td>The platform supports workflow, dashboarding and communication functionalities</td>
<td>Pick and choose modules based on your requirements</td>
<td>DPO One is cloud-based and will be hosted in the Microsoft Azure environment</td>
</tr>
</tbody>
</table>

**DPO One**

- **Dashboarding**
- **Modules**
- **Intelligence**
- **DPO One Support**

---

#### The various GDPR requirements are embedded within the DPO One modules

<table>
<thead>
<tr>
<th>Advanced dashboards</th>
<th>Reporting</th>
<th>Advanced reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data retention</td>
<td>Consent &amp; information provisioning</td>
<td>Advanced vendor &amp; processing management</td>
</tr>
<tr>
<td>Advanced privacy by design</td>
<td>Advanced data security</td>
<td>Data subject request (front end)</td>
</tr>
<tr>
<td>Advanced data security</td>
<td>Advanced international data transfers</td>
<td>Advanced e-learning platform</td>
</tr>
<tr>
<td>Data discovery</td>
<td>Cookies</td>
<td></td>
</tr>
</tbody>
</table>

**Standard Modules**

<table>
<thead>
<tr>
<th>DPO one support</th>
<th>ROPA</th>
<th>Data subject request</th>
<th>Supervisory authority support</th>
<th>Privacy by design</th>
<th>International data transfers</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPO one essentials</td>
<td>PIA</td>
<td>Control framework &amp; testing</td>
<td>Data breach</td>
<td>E-learning &amp; awareness</td>
<td>Data security</td>
</tr>
<tr>
<td>Risk register</td>
<td>Dashboard</td>
<td>Reporting</td>
<td>Security</td>
<td>Privacy</td>
<td>Data transfers</td>
</tr>
</tbody>
</table>
Incident reporting

Mandatory breach notification

One of the key changes the GDPR introduces is that organizations must notify the supervisory authority of data breaches ‘without undue delay’, within 72 hours, unless the breach is unlikely to be a risk to individuals. If there is a high risk to individuals, those individuals must be informed as well.

During the 72 hours after a data breach has been discovered, an organization must:

- Carry out a thorough investigation
- Inform regulators and impacted individuals of the breach
- Identify what personal data has been impacted and how
- Draft a comprehensive containment plan

...and all of this within 72 hours.

If a notification is not made within the 72-hour window, the GDPR requests that the controller provides reasonable justification for the delay; potentially adding additional disruption to regular business operations and exasperating administrative hassle.

GDPR specifies what type of information the notification must include. At a minimum, the data protection authority will expect to see:

- Nature of Breach
  1. Who accessed what and when
  2. Who are these users
  3. How is that data being used
  4. Impacted individuals
- Record of work that has been done to prevent a breach
- Estimated impact of the breach
- Forensics details
- Communication support
- Legal support
- Notify authorities within 72 hours and affected individuals without undue delay
- Mitigation or remediation plan

EY offers a unique service that covers the Incident and Breach Management, helping the organization to meet the GDPR requirements while supporting client to simultaneously address the issues associated with the breach and maintain ongoing operations. EY’s Data Incident Response Plan will not only support the client in the crucial 72-hour operational effectiveness process, but also help to identify and distinguish whether the company was a victim of a cyber-attack or a solely data attack. EY will provide the necessary support to the organization in both cases accordingly.
Practice making decisions in a simulated crisis

While some types of crises are predictable in the generic sense, each one has its own distinct characteristics. Moreover, inevitably, the crisis that hits the hardest is the one a firm doesn't expect. Building top executives' experience in making decisions in crisis is vital. Firms often conduct tactical simulations or tabletop exercises lower down the organization, on liquidity or cyber, but it is important that these simulations are also undertaken at the most senior levels of the firm, so leaders know how they should operate in crisis. Such simulations often help firms determine how they would react for specific crises, e.g., how they would respond to a data breach or prolonged outage involving a key vendor.
Where we are currently helping out clients?

**Data Protection Officer (DPO)**
- Support of existing DPOs and help with choosing and training future DPOs
- Guidance on matters related to data protection and processing operations

**Assurance & Attestation (SOCR, Independent Reviews)**
Provide the formal GDPR attestation reporting and other independent reviews to support clients on their path to full GDPR compliance.

We intend to become certification body in due course under CNPD’s CARPA certification mechanism framework.

**Breach Management Support**
Support maturity of client’s crisis management, incident management and cyber breach response through:
- Gap assessment on breach readiness
- Design & implementation
- Assess severity and breach impact
- Validation of breach process

**Privacy Programme Support**
Privacy programme & subject matter support
- Privacy Strategy
- Establishing Compliance programme
- Running privacy programme
- Crisis Management
- Vendor Due Diligence
- PIAs, Data Discovery, SARs, RoPA, Training

**Regulatory Action Support**
- Provide support in meeting requests from Supervisory Authorities (SA)
- Assist with preparatory work prior to visits from SAs
**GDPR Maturity Assessment/Benchmark**

Benchmark of the GDPR maturity of the organization as they continue to establish their response to the legislation.

**Internal Audit**

Supporting clients on internal audit reviews and help to streamline privacy audits with analytics and RPA.

**Vendor due diligence, GDPR Supply chain assurance**

Assess a controller's compliance to contract and or compliance to GDPR

Or benchmark ongoing maturity of the controller.

**GDPR Compliance Audit/Assessment**

Detailed assessment/audit of the organization's compliance to the GDPR - To identify and assess the controls that have been established to (PbD) mitigate the risk of a data loss

**BCR Review & Readiness**

- Review of the organization's existing BCR/SCC framework
- Conduct readiness assessment of the controls required to develop the BCR/SCC
- Assist with the authorization procedure of the BCR

**DPO One**

DPO One is a platform supporting GDPR management processes including:

- Intelligence
- Workflow
- Risk dashboard
- SME and Managed services
Contact us

To find out more about our privacy-related services and how can EY help you use GDPR as a catalyst for change, beyond compliance, please contact:

**Michael Hofmann**  
Partner, Advisory Services, GDPR Leader, Cyber Security  
+352 42 124 8895  
michael.hofmann@lu.ey.com

**Olivier Maréchal**  
Partner, Financial Services Advisory Leader  
+352 42 124 8948  
olivier.marechal@lu.ey.com

**Patrice Fritsch**  
Principal, Managed Services  
+352 42 124 8950  
patrice.fritsch@lu.ey.com

**Alexandre Minarelli**  
Director, IT Risk & Assurance Leader, Commercial and Public Sector  
+352 42 124 8669  
alexandre.minarelli@lu.ey.com

**Alejandro Del Río**  
Manager  
+352 42 124 8301  
alejandro.del-rio@lu.ey.com
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.

© 2019 Ernst & Young Business Advisory Services S. à R. L.
All Rights Reserved.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/luxembourg