

# **EU General Data Protection Regulation: are you ready?**



# Contents

What you need to know about the new EU General Data Protection Regulation	2
Is your organization ready for the EU General Data Protection Regulation?	4
Findings from the joint IAPP and EY Privacy Governance Report 2016	5
How EY can help you prepare	6
Example outputs	8
Contacts	9





# What you need to know about the new EU General Data Protection Regulation

Data protection has entered a period of unprecedented change.

This has been driven by:

1.

An increasing number of high-profile data breaches reported in the media that have led consumers and regulators to be concerned about how personal data is managed

2.

The demise of safe harbor

3.

The new European Union (EU) General Data Protection Regulation (GDPR) – a landmark moment in data protection

On 17 December 2015, after more than three years of tough negotiations and several draft versions of the GDPR, an informal agreement was reached between the European Parliament and the Council of the EU. The GDPR is a game changer for organizations. It introduces more stringent and prescriptive data protection compliance challenges, backed by fines of up to 4% of global annual revenue. The regulation replaces the Directive 95/46/EC, which has been the basis of European data protection law since it was introduced in 1995.

The regulation has a significant impact on businesses in all industry sectors, bringing with it both positive and negative changes for business in terms of cost and effort. Organizations are likely to welcome the harmonization of laws across the 28 Member States which will make the complex data protection landscape easier to navigate for multinational organizations. The introduction of new rights for individuals, such as the right to be forgotten and the right to portability, as well as the introduction of mandatory breach notification requirements, are likely to increase the regulatory burden

for organizations. Businesses need to review their current data protection compliance programs to determine next steps and decide on the level of investment they need to make before 2018 to address the changes.

Organizations need to act now to ensure that they are ready to comply with the new regulation when it comes into force on 25 May 2018.





## Key changes proposed by the GDPR

### Fines of up to 4% of annual worldwide turnover

Fines for a breach of the GDPR are substantial. Regulators can impose fines of up to 4% of total annual worldwide turnover or €20,000,000

### Expanded scope

The new regulation applies to all data controllers and processors established in the EU and organizations that target EU citizens.

### Data protection officers (DPOs)

DPOs must be appointed if an organization conducts large-scale systematic monitoring or processes large amounts of sensitive personal data.

### Accountability

Organisations must prove they are accountable by:

- ▶ Establishing a culture of monitoring, reviewing and assessing data processing procedures
- ▶ Minimizing data processing and retention of data
- ▶ Building in safeguards to data processing activities
- ▶ Documenting data processing policies, procedures and operations that must be made available to the data protection supervisory authority on request

### Privacy impact assessments

Organizations must undertake Privacy impact assessments when conducting risky or large-scale processing of personal data.

### Consent

Consumer consent to process data must be freely given and for specific purposes. They also must be informed of their right to withdraw their consent. The consent must be “explicit” in the case of sensitive personal data or transborder data flow.

### Mandatory breach notification

Organizations must notify supervisory authority of data breaches “without undue delay” or within 72 hours, unless the breach is unlikely to be a risk to individuals. If there is a high risk to individuals, they must also be informed.

### New rights

- ▶ The right to be forgotten, meaning the right to ask data controllers to erase all personal data without undue delay in certain circumstances
- ▶ The right to data portability. Where individuals have provided personal data to a service provider, they can require the provider to “port” the data to another provider, provided this is technically feasible.
- ▶ The right to object to profiling, i.e., the right not to be subject to a decision based solely on automated processing.

### Privacy by design

Organizations should design data protection into the development of business processes and new systems. Privacy settings are set at a high level by default.

### Obligations on processors

The new regulation entails new obligations on data processors. Processors become an officially regulated entity.

# Is your organization ready for the EU General Data Protection Regulation?

Now is the time to take action. Areas of consideration are as follows:

## **Expanded scope**

Are you a data processor or a data controller processing personal data inside the EU or processing the personal data of EU citizens?

## **DPOs**

Do you conduct large-scale systematic monitoring (including employee data) or process large amounts of sensitive personal data?

## **New rights**

Do you know how you will comply with the new rights: the right to be forgotten, the right to data portability and the right to object to profiling?

## **Accountability**

Do you have a data protection programme and are you able to provide evidence of how you comply with the requirements of the GDPR?

## **Privacy by design**

Do you design data protection and privacy requirements into the development of your business processes and new systems?

## **Mandatory breach notification**

Would you be able to notify a data protection supervisory authority of a data breach within 72 hours?

# Findings from the joint IAPP and EY Privacy Governance Report 2016

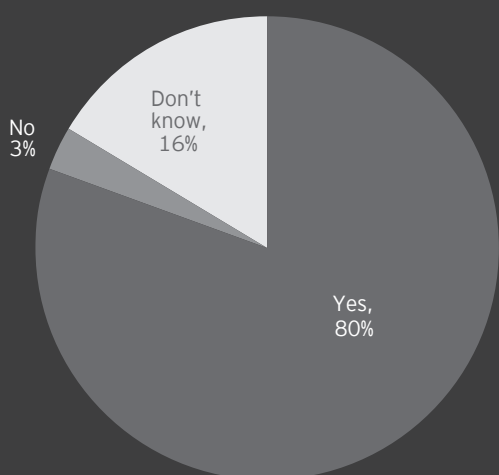
Source: <https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2016/>.

## Key finding from the report: 8 in 10 organizations who transfer data say they fall under GDPR

Our report indicates that three aspects of the GDPR are considered most difficult: the right to be forgotten, data portability and explicit consent requirements.

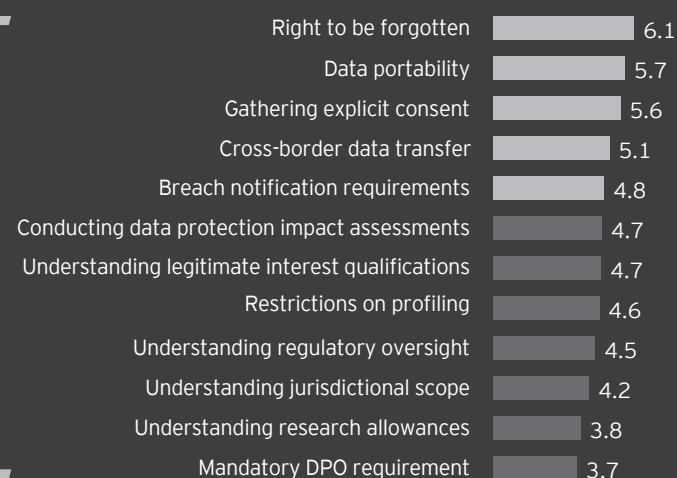
Does your organization fall under the scope of the GDPR?

### Whether Fall Under GDPR Scope, Among Those Who Transfer



Please rate each of the following legal obligations of the GDPR on a scale from 0 to 10

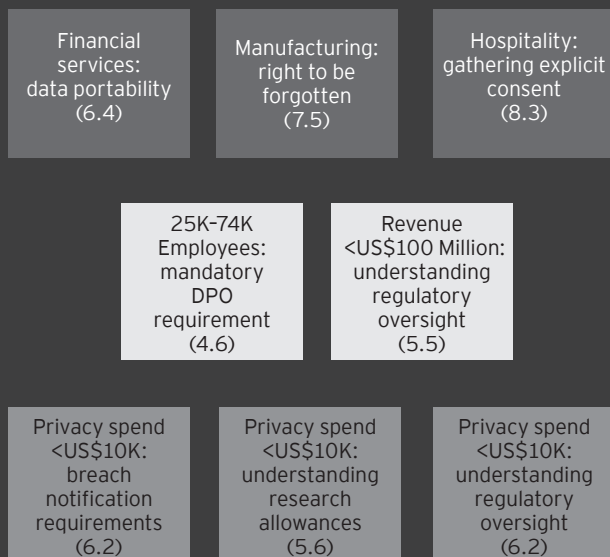
### GDPR obligation difficulty (Mean Score On 0-10 Scale: 0 = Not At All Difficult; 10 = Extremely Difficult)



Our report indicates that several GDPR obligations are of higher-than-average concern to certain segments.

### GDPR obligation difficulty: higher-than-average concerns

(Mean score on 0-10 Scale: 0 = Not At All Difficult; 10 = Extremely Difficult)



Our report indicates that the most commonly taken step to prepare for the GDPR is developing training and accountability frameworks.

About one-third say they are preparing by boosting their privacy budget or privacy staff.

### Steps being taken to prep for the GDPR (Among those falling under the GDPR)



# How EY can help you prepare

Action	Overview	Scope	Timescales
GDPR targeted assessment	High-level assessment of data protection maturity	<ul style="list-style-type: none"> <li>▶ Targeted assessment gauging readiness for the new requirements of the GDPR</li> </ul>	One day
GDPR “360 Degree” assessment	Detailed assessment of data protection maturity Compliance requirements Risk assessments	<ul style="list-style-type: none"> <li>▶ Risk assessment and maturity evaluation based on industry framework and GDPR</li> <li>▶ Recommendations and road map for remediation</li> <li>▶ Product- and process-specific risks</li> </ul>	Two to four weeks, depending on the size and complexity of the organization
Privacy Impact Assessment	Customized Privacy Impact Assessment	<ul style="list-style-type: none"> <li>▶ Assessment of your systems or projects identifying key data protection risks</li> </ul>	One to two weeks, depending on the size and complexity of the project or systems that need to be analyzed
“Know your personal data” – data inventory	Personal information inventory Personal information flow documentation	<ul style="list-style-type: none"> <li>▶ Use of the data inventory tool to identify and document a sample of the personal data you have in your organization, where it is, where is transferred from and to, and who has access to it</li> <li>▶ Process- or system-specific personal information flow diagrams and documentation</li> </ul>	Between 1 and 12 weeks, depending on the size and complexity of the organization

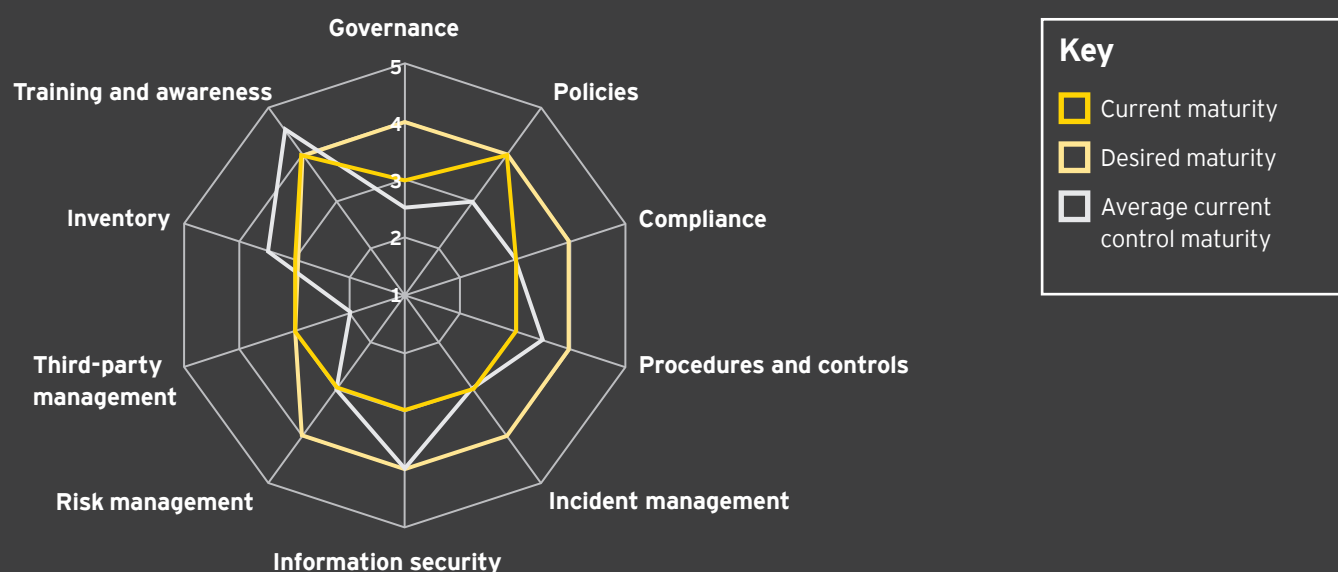




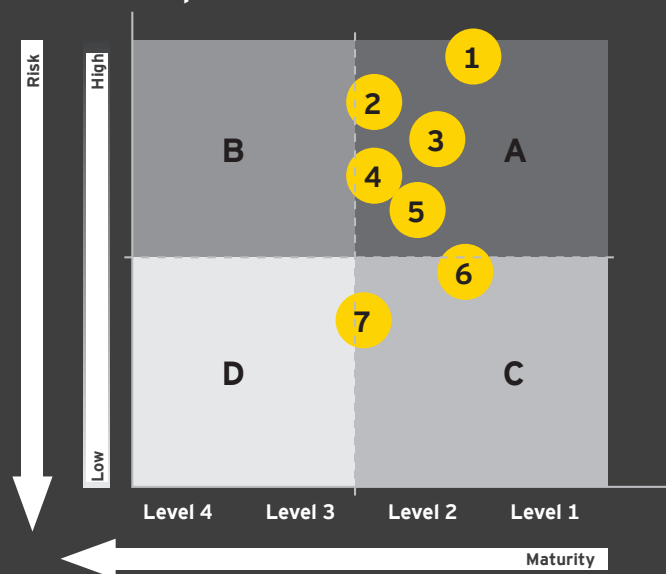
Services	Overview	Service provider	Timescales
Data protection improvement programme	Programme design	Design and assistance of data protection improvement programs, including the development and implementation of: <ul style="list-style-type: none"> <li>▶ Data protection frameworks</li> <li>▶ Privacy governance and organization design</li> <li>▶ Policy and procedures</li> <li>▶ Training and awareness</li> <li>▶ Incident management</li> <li>▶ Third-party management</li> <li>▶ Risk management</li> <li>▶ Procedures and controls</li> <li>▶ Information security controls</li> <li>▶ Binding corporate rules program compliance</li> <li>▶ Ongoing compliance and monitoring</li> </ul>	Between 3 and 24 months, depending on maturity and size of the organization
	Programme implementation		
	Compliance and monitoring solutions		
	Ongoing Programme support		
Legal support	Legal analysis	<ul style="list-style-type: none"> <li>▶ Legal analysis of compliance with data protection legislation</li> <li>▶ Drafting and advising on compliance programs and policies</li> <li>▶ Assessment of any non-compliance and suggestions of remedial action</li> <li>▶ Drafting for data controller and data processor agreements</li> <li>▶ Drafting of Binding corporate rules</li> </ul>	Assessed on a case-by-case basis, depending on scope
	Drafting of legal documents		

# Example outputs

We can work with organisations to help enhance their understanding of their compliance position and maturity level. Below are some examples of the types of work products we have previously produced on data protection engagements.



EY's risk map



## Key

### Circles

1. Third-party management
2. Training and awareness
3. Risk management
4. Policy
5. Data leakage
6. Treating customer fairly
7. Incident management

### Sectors

- A. Higher risk, lower maturity
- B. Higher risk, higher maturity
- C. Lower risk, lower maturity
- D. Lower risk, higher maturity

Organizations face many challenges in preparing for the GDPR before it comes into force in May 2018. It is important that they understand their current state and the steps necessary to move toward compliance with the GDPR.



# EY contacts

To discuss any of these issues or for further information, please contact:



**Fabrice Naftalski**

Global Head of Data Protection  
and IP/IT Law

Tel: +33 1 5561 1005

Mobile: +33 60770 8758

Email: [fabrice.naftalski@ey-avocats.com](mailto:fabrice.naftalski@ey-avocats.com)



**Dr. Peter Katko**

Global Digital Law Leader  
Ernst & Young Law GmbH  
Rechtsanwaltsgesellschaft  
Steuerberatungsgesellschaft

Tel: +49 89 14331 25951

Mobile: +49 160 939 25951

Email: [peter.katko@de.ey.com](mailto:peter.katko@de.ey.com)



**Tony De Bos**

EMEIA Data Protection & Privacy Financial  
Services Leader

Tel: +31 88 407 20797

Mobile: +31 62908 4182

Email: [tony.de.bos@nl.ey.com](mailto:tony.de.bos@nl.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](https://ey.com).

EY member firms do not provide advice on US law.

© 2017 EYGM Limited.  
All Rights Reserved.

EYG no. 01015-172GBL

BMC Agency  
GA 0000\_10165

ED None

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**