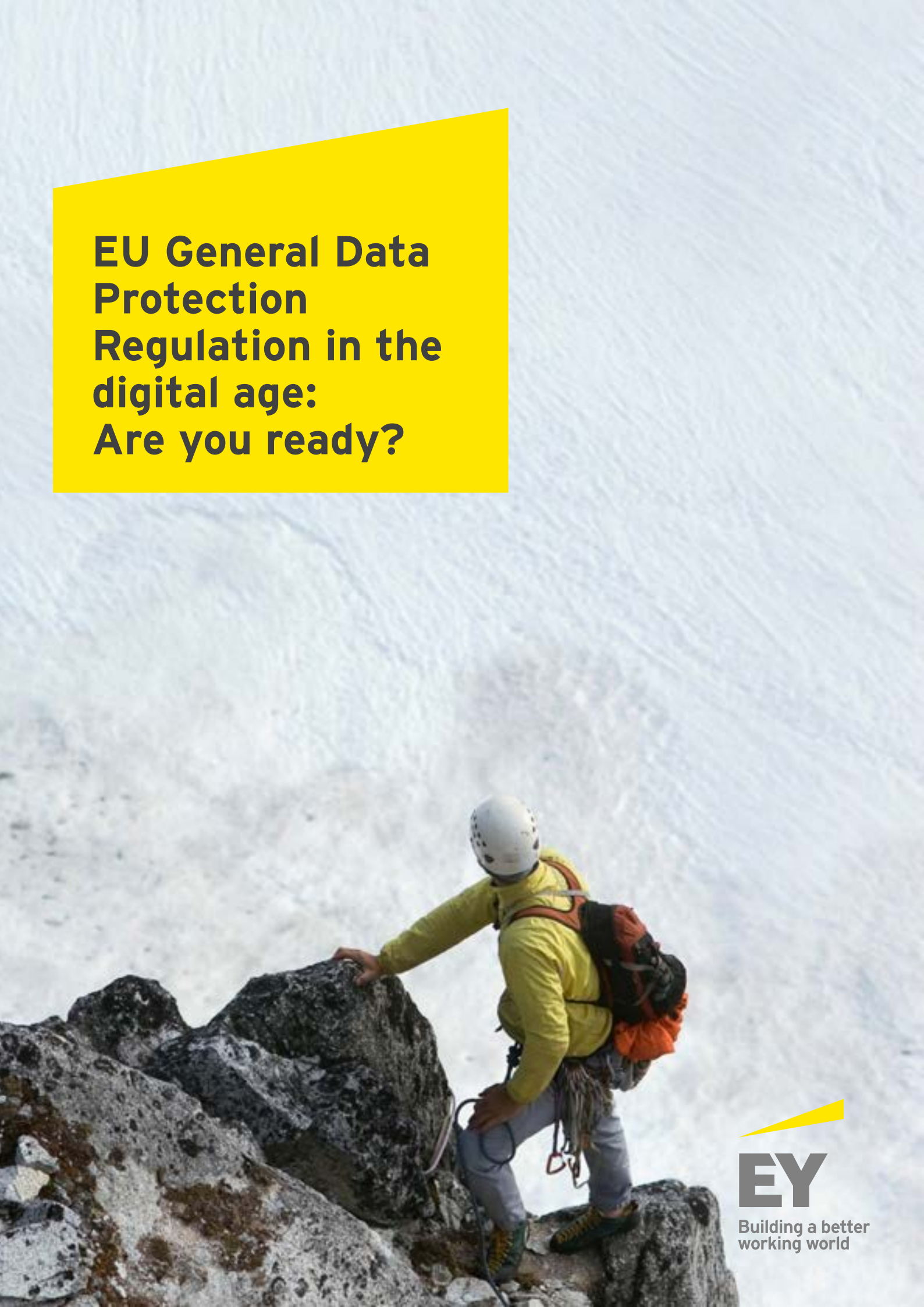
EU General Data Protection Regulation in the digital age: Are you ready?



EY
Building a better working world

What do 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:

- An increasing number of high profile data breaches reported in the media that has led consumers and regulators to be concerned about how personal data is managed
- The demise of Safe Harbor
- The new EU General Data Protection Regulation (GDPR) – a landmark moment in data protection

On May 4, 2016, after four years of tough negotiations, the GDPR has now been published in the Official Journal. The regulation is a game changer for organisations. The final draft introduces more stringent and prescriptive data protection compliance challenges, backed by fines of up to 4% of global annual revenue. The Regulation will replace the Directive 95/46/EC, which has been the basis of European data protection law since it was introduced in 1995. The GDPR will enter into force in EU Member States on 25 May 2018.

The Regulation will have 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. Organisations are likely to welcome the harmonisation of laws across the 28 member states which will make the complex data protection landscape easier to navigate for multinational organisations. 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, are likely to increase the regulatory burden for organisations. Businesses need to review their current data protection compliance programmes to determine next steps and decide on the level of investment they need to make over the next two years to address the changes.

Organisations need to act now to ensure that they are ready to comply with the new Regulation when it comes into force in May 2018.

Key changes proposed by the EU 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	Applies to **all data controllers and processors established in the EU** and organisations that **target EU citizens**
Data Protection Officers (DPOs)	DPOs must be appointed if an organisation conducts **large scale systematic monitoring** or processes **large amounts of sensitive personal data**
Accountability	Organisation must prove they are **accountable** by: ► Establishing a culture of **monitoring, reviewing and assessing** data processing procedures ► **Minimising** 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	Organisations 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** ► Customers must be **informed of their right to withdraw** their consent ► Consent must be **'explicit'** in the case of sensitive personal data or transborder dataflow
Mandatory breach notification	► Organisations 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, those **individuals must be informed** as well
New rights	► The **right to be forgotten** – 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
Privacy by Design	► Organisations 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	► **New obligations on data processors** – processors become an officially regulated entity
Joint controllers	► Data protection responsibility might split among several controllers

Are organisations ready for the EU General Data Protection Regulations?

Organisations will have **two years** to prepare for the GDPR in the transition period between national laws under the old directive and the new regulation.

Now is the time to take action.

Ask yourself these key questions:

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?
Data Protection Officers	Do you conduct large scale systematic monitoring (including employee data) or process large amounts of sensitive personal data?
Accountability	Do you have a data protection programme and are you able to provide evidence of how you comply with the requirements of the EU GDPR?
Mandatory Breach Notification	Would you be able to notify a data protection supervisory authority of a data breach within 72 hours?
Privacy by Design	Do you design data protection and privacy requirements into the development of your business processes and new systems?
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'?
Consent and Notice	Do your data protection terms comply with the new requirements on consent (unambiguous) and notice (legitimate interest)?

Findings from the joint **IAPP-EY Annual Privacy Governance Report 2015** and **the EY Global Information Security Survey 2015** both indicated that organisations still need to increase their investment in data protection.

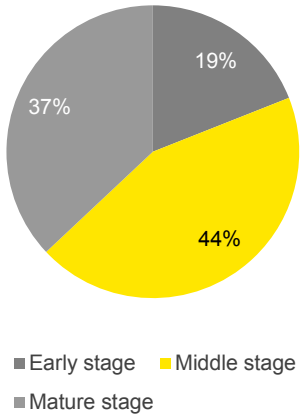
- Both reports identified that data protection is not yet a high priority
- 63% of respondents from the IAPP-EY Annual Privacy Governance report highlighted that their privacy maturity was only at early or middle stages of maturity

Organisations will need to increase their focus on data protection compliance given the stringent requirements of the GDPR and the potential fines which can be up to 4% of an organisations global annual turnover.

The new EU GDPR is driving organisations to invest in privacy programmes:

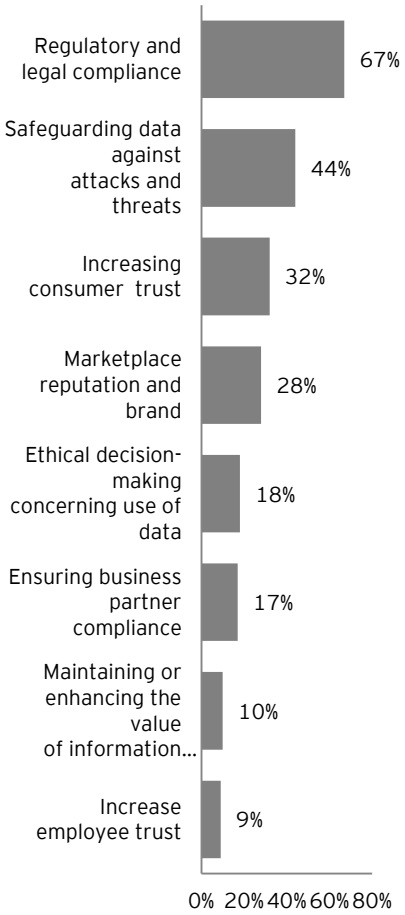
- 67% of organisations interviewed for the IAPP-EY Annual Privacy Governance Report 2015 said that regulatory and legal compliance was one of their top reasons for investing in privacy
- 31% of organisations are planning to increase the number of employees dedicated to their privacy programmes and increase privacy budgets in the coming year

Where is privacy maturity process in your company?

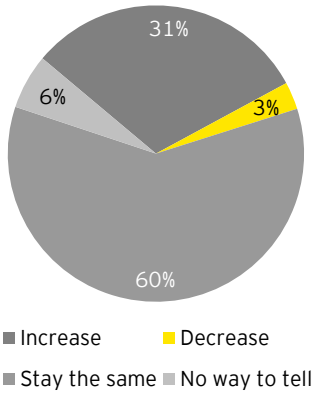


Mean number of years for the duration of a privacy programme = 7

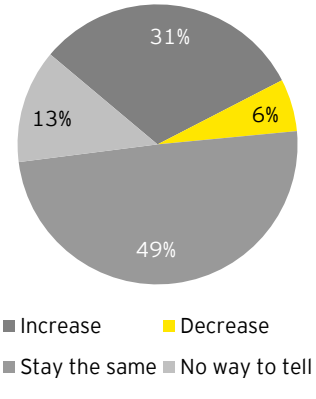
Privacy program priorities
(% ranking each in top two)



In the coming year, number of employees dedicated to privacy is expected to:



In the next 12 months, expect privacy budget will:



Source: The IAPP-EY Annual Privacy Governance Report 2015

How can you prepare for the EU General Data Protection Regulation?

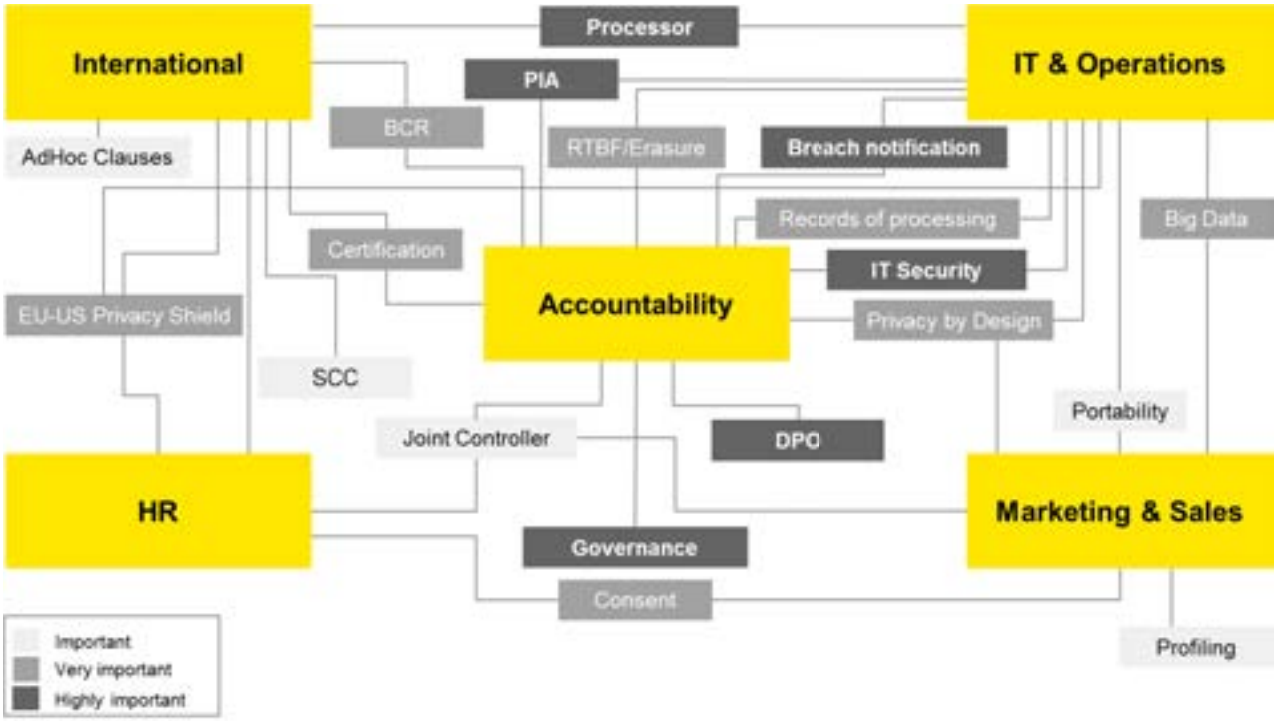
To prepare for the new EU GDPR, organisations will need to have a clear understanding of their current compliance position.

An important first step will be for organisations to have clarity of their personal data processing, including:

- **What** personal data they process
- **Where it is** across their organisation
- **Where it is transferred** from and to (including to third parties and cross-border)
- **How it is secured** throughout its lifecycle

Following that organisations shall analyse the relevance of the new requirements under the GDPR for the different risk areas. With an understanding of their compliance gaps, organisations will be in a position to assess their personal data risks and develop prioritised remediation plans in order to adjust their data protection management to the new landscape under the GDPR .

The data protection landscape under the GDPR



EY GDPR solutions

GDPR Speed Assessment

How do we do it?

1:1 meeting using our speed assessment tool to walk through your current compliance with the new GDPR and identify significant gaps and remediation required.

What do you get?

A targeted and quick assessment of your compliance with the GDPR, providing a dashboard showing your readiness to comply with each of the key GDPR requirements.

GDPR '360 Degree' assessment

How do we do it?

Detailed questionnaires, interviews and workshops to understand your GDPR compliance position.

What do you get?

A detailed assessment showing your maturity against the GDPR requirements, your key gaps and risks, and a remediation roadmap.

Privacy Impact Assessments (PIA)

How do we do it?

Design of a tailored PIA template. Interviews with system/project owners and review of designs and documentation to assess the risks of harm to individuals through the misuse of their personal information.

What do you get?

A detailed assessment of your systems or projects identifying key privacy risks and remediation required to produce compliant methods for handling personal information.

International data transfer strategy

How do we do it?

Design of the appropriate data transfer tool based in the analysis of the relevant data flows.

What do you get?

Customized and flexible framework which enables to continuously update triggered by new applications or new entities adhering to the system.

GDPR Compliance Toolkit

How do we do it?

A programme of interlinked activities to develop your privacy framework and improve your maturity and compliance with the GDPR.

What do you get?

Development and implementation of a robust data protection framework, remediating your GDPR compliance gaps.

Legal advice and support

How do we do it?

Global network of lawyers with cross border expertise, on hand to provide tailored legal advice and solutions.

What do you get?

Legal advice tailored to the needs of your organisation. If requested also EY Law acting as data protection officer

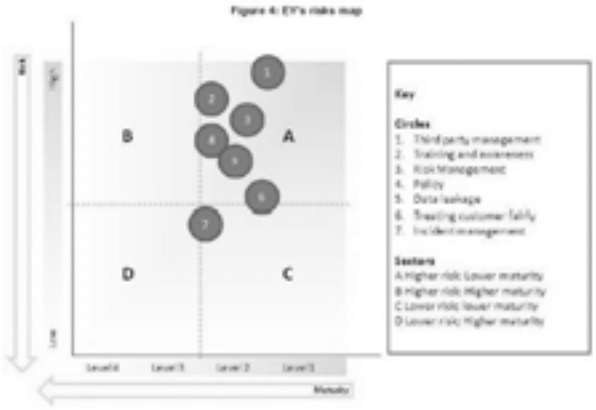
How we can help you get ready

Solution	Overview	Service provided	Timescales
GDPR Speed Assessment	High level assessment of data protection maturity	► Targeted assessment gauging readiness for the new requirements of the GDPR	1 day
GDPR '360 Degree' Assessment	Detailed assessment of data protection maturity Risk assessments	► Risk assessment and maturity evaluation based on industry framework and EU General Data Protection Regulation ► Recommendations and roadmap for remediation ► Product and process-specific risks	2-4 weeks depending on the size and complexity of the organisation
Privacy Impact Assessment	Customised Privacy Impact Assessment	► Assessment of your systems or projects identifying key data protection risks	1-2 weeks depending on the size and complexity of the process or system
International data transfer strategy	Standard Contractual Clauses Binding Corporate Rules Other tools such as codes of conducts or EU-US Privacy Shield	► Identification of data flows ► Design of the appropriate data transfer tool, including the development and implementation of: ► Standard contractual clauses (for data controllers or data processors) ► BCRs ► Policy and procedures (such as audit program, internal compliance management…) ► Privacy governance and organization design ► Codes of conducts ► EU-US Privacy Shield	1-24 months depending on the size of the entity and the tools to be implemented

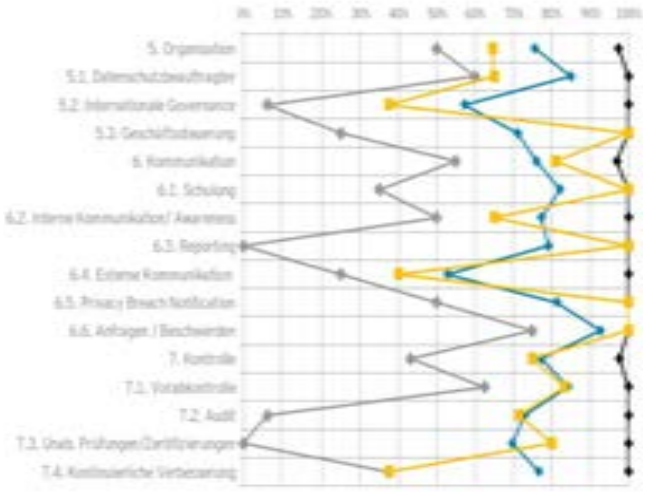
Solution	Overview	Service provided	Timescales
GDPR Compliance Toolkit	Mapping of applicable legal requirements Compliance and legal monitoring solutions Documentation of data processing operations Drafting and implementation of procedures and policies	► Design and delivery of data protection improvement programmes, including the development and implementation of: ► Data protection frameworks ► Privacy governance and organisation design ► Policy and procedures ► Training and awareness ► Incident management ► Third Party management ► Risk management ► Procedures and controls ► Information security controls ► Binding Corporate Rules program compliance ► Ongoing compliance and monitoring	3-24 months depending on maturity and size of the organisation
DPO Legal Support	Legal analysis and drafting of legal documents EY acting as external DPO	► Legal analysis of compliance with data protection legislation ► Assessment of any non-compliance and suggestions of remedial action ► Drafting for data controller and data processor agreements ► Training of DPO ► EY Law as DPO	Assessed on a case by case basis – depending upon scope

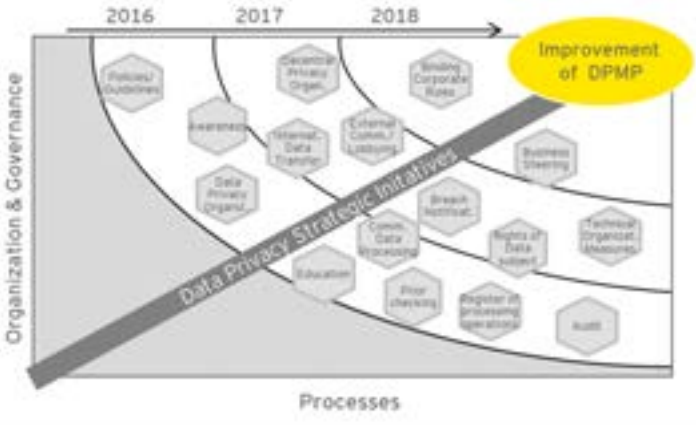
Example outputs

We can work with organisations to 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:



Strategy to improve data privacy management system





1

Organisations face many challenges preparing for the EU GDPR over the next couple of years. It is important that they understand their current state and the steps necessary to move towards compliance with the EU GDPR.

If you would like to discuss any of the issues raised in this brochure then please get in touch with the contacts overleaf.

EU General Data Protection Regulation: Get ready, the clock is ticking

Contacts

Dr. Peter Katko
Partner, Global Digital Law Leader
Phone +49 89 14331 25951
Fax +49 181 3943 25951
Mobile +49 160 939 25951
peter.katko@de.ey.com

Daniel Kaiser
Senior Manager, Privacy Law
Phone +49 89 14331 13001
Fax +49 181 3943 13001
Mobile +49 160 939 13001
daniel.kaiser@de.ey.com

Monika Menz
Senior Manager, Privacy Law
Tel +49 30 25471 10027
Mobil +49 160 939 10027
Fax +49 181 3943 10027
E-Mail monika.menz@de.ey.com

EY | Assurance | Tax | Transactions | Advisory

About the global EY organization
The global EY organization is a leader in assurance, tax, transaction and advisory services. We leverage our experience, knowledge and services to help build trust and confidence in the capital markets and in economies the world over. We are ideally equipped for this task – with well trained employees, strong teams, excellent services and outstanding client relations. Our global purpose is to drive progress and make a difference by building a better working world – for our people, for our clients and for our communities.

The global EY organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity's acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information, please visit www.ey.com.

In Germany, EY has 22 locations. In this presentation, "EY" and "we" refer to all German member firms of Ernst & Young Global Limited.

www.de.ey.com

In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.