EU General Data Protection Regulation: Are you ready?
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What do you need to know about the new EU General Data Protection Regulation?</td>
<td>2</td>
</tr>
<tr>
<td>Are organisations ready for the EU General Data Protection Regulations?</td>
<td>4</td>
</tr>
<tr>
<td>How can you prepare for the EU General Data Protection Regulation?</td>
<td>6</td>
</tr>
<tr>
<td>How we can help you get ready</td>
<td>8</td>
</tr>
<tr>
<td>Example outputs</td>
<td>10</td>
</tr>
<tr>
<td>Contacts</td>
<td>12</td>
</tr>
</tbody>
</table>
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:

1. 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

2. The demise of Safe Harbor

3. The new EU General Data Protection Regulation (GDPR) - a landmark moment in data protection

On December 17, 2015, after more than three years of tough negotiations and several draft versions of the GDPR, an informal agreement has been reached between the European Parliament and Council of the European Union. The GDPR is a game changer for organisations. The final draft has been backed by the Committee on Civil Liberties, Justice and Home Affairs. It 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. When the GDPR is officially adopted later this year it will apply in EU Member States without further consultation after a period of two years.

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 the spring of 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  
| • The right to object to profiling – the right not to be subject to a decision based solely on automated processing |
| **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 |
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 the old directive and the new regulation.

Now is the time to take action.

**Ask yourself these key questions:**

<table>
<thead>
<tr>
<th>Expanded scope</th>
<th>Data Protection Officers</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you a data processor or a data controller processing personal data inside the EU or processing the personal data of EU citizens?</td>
<td>Do you conduct large scale systematic monitoring (including employee data) or process large amounts of sensitive personal data?</td>
<td>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?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mandatory Breach Notification</th>
<th>Privacy by Design</th>
<th>New rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you be able to notify a data protection supervisory authority of a data breach within 72 hours?</td>
<td>Do you design data protection and privacy requirements into the development of your business processes and new systems?</td>
<td>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’?</td>
</tr>
</tbody>
</table>
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 organisation’s global annual turnover.

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?

- Early stage: 37%
- Middle stage: 19%
- Mature stage: 44%

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

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

- Increase: 6%
- Decrease: 31%
- Stay the same: 31%
- No way to tell: 6%

In the next 12 months, expect privacy budget will:

- Increase: 31%
- Decrease: 13%
- Stay the same: 6%
- No way to tell: 49%

Privacy program priorities (% ranking each in top two)

- Regulatory and legal compliance: 67%
- Safeguarding data against attacks and threats: 44%
- Increasing consumer trust: 32%
- Marketplace reputation and brand: 28%
- Ethical decision-making concerning use of data: 18%
- Ensuring business partner compliance: 17%
- Maintaining or enhancing the value of information: 10%
- Increase employee trust: 9%

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.

With an understanding of their compliance gaps, organisations will be in a position to assess their personal data risks and develop prioritised remediation plans.

EY is helping clients address these challenges with the following solutions:

- **GDPR Readiness Assessment**
  Workshops and 1:1 meeting to establish key GDPR gaps

- **GDPR ‘360 Degree’ Assessment**
  Detailed assessment of maturity and compliance with the GDPR

- **Privacy Impact Assessments (PIA)**
  Assessments of privacy risk across new systems or projects

- **‘Know your personal data’**
  Identify where personal data is across your network and create a personal data inventory using tooling, e.g., the Raven Exonar tool

- **Data protection improvement programme**
  Holistic programme to achieve compliance with the GDPR
# GDPR Readiness Assessment

**How do we do it?**
Workshops and 1:1 meeting using our Readiness 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.

---

# ‘Know your personal data’ – data inventory

**How do we do it?**
Use the Exonar Raven platform to scan an agreed sample of your network and interrogate the contents of documents to understand what personal data you have in your organisation and where it is.

**What do you get?**
A personal data inventory, dashboard and a data map of the data analysed enabling you to have a clear picture of the personal data you use across your organisation.

---

# Data protection improvement programme

**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.
# How we can help you get ready

<table>
<thead>
<tr>
<th>Solution</th>
<th>Overview</th>
<th>Service provider</th>
<th>Timescales</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR Targeted Assessment</td>
<td>High level assessment of data protection maturity</td>
<td>► Targeted assessment gauging readiness for the new requirements of the GDPR</td>
<td>1 day</td>
</tr>
</tbody>
</table>
| GDPR ‘360 Degree’ Assessment          | Detailed assessment of data protection maturity                          | ► Risk assessment and maturity evaluation based on industry framework and EU General Data Protection Regulation  
                                         | Compliance requirements                                                   | ► Recommendations and roadmap for remediation                                   | 2-4 weeks depending on the size and complexity of the organisation     |
|                                       | Risk assessments                                                         | ► Product and process-specific risks                                              |                                                                           |
| 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 organisation        |
| ‘Know your personal data’ - data inventory | Personal information inventory                                           | ► Use of the Exonar Raven tool to identify and document a sample of the personal data you have in your organisation, where it is, where is transferred from/to, who has access to it  
<pre><code>                                     | Personal Information flow documentation                                    | ► Process or system specific personal information flow diagrams and documentation | 2-12 weeks depending on the size and complexity of the organisation     |
</code></pre>
<table>
<thead>
<tr>
<th>Solution</th>
<th>Overview</th>
<th>Service provider</th>
<th>Timescales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection improvement programme</td>
<td>Programme design</td>
<td>Design and delivery of data protection improvement programmes, including the development and implementation of:</td>
<td>3-24 months depending on maturity and size of the organisation</td>
</tr>
<tr>
<td></td>
<td>Programme implementation</td>
<td>► Data protection frameworks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance and monitoring solutions</td>
<td>► Privacy governance and organisation design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ongoing Programme support</td>
<td>► Policy and procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Training and awareness</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Incident management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Third Party management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Risk management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Procedures and controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Information security controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Binding Corporate Rules program compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Ongoing compliance and monitoring</td>
<td></td>
</tr>
<tr>
<td>Legal Support</td>
<td>Legal analysis</td>
<td>► Legal analysis of compliance with data protection legislation</td>
<td>Assessed on a case by case basis - depending upon scope</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Drafting and advising on compliance programmes and policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Assessment of any non-compliance and suggestions of remedial action</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Drafting for data controller and data processor agreements</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Drafting of Binding Corporate Rules</td>
<td></td>
</tr>
</tbody>
</table>
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:

- Training and Awareness Policies
- Inventory Compliance
- Governance
- Third Party Management
- Procedures and Controls
- Risk Management
- Incident Management
- Information Security

GeoLocation of SPI/PII Data Outside the UK

[Map showing GeoLocation of SPI/PII Data Outside the UK]
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.

**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

---

1 Images from Raven Exonar
Contacts

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

**Chris Gould**  
Partner, Cyber Security  
and Resilience  
Tel: +44 20 7951 0086  
Mobile: +44 7831 136 995  
Email: cgould@uk.ey.com

**Nicola Hermansson**  
Director, UK&I Data  
Protection Leader  
Tel: +44 20 7951 8332  
Mobile: +44 7795 828 811  
Email: nhermannsson@uk.ey.com

**Louisa Elder**  
Director, Head of IP and Data  
for Law  
Tel: +44 20 7197 7929  
Mobile: +44 7714 204 208  
Email: lelder@uk.ey.com
EU General Data Protection Regulation: Get ready, the clock is ticking
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.

Ernst & Young LLP
The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.
© 2016 Ernst & Young LLP. Published in the UK.
All Rights Reserved.
ED None
1411555.indd (UK) 03/16. Artwork by Creative Services Group Design.

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.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com/uk