GDPR: THE BIG PICTURE

John Bowman
Senior Principal
Promontory, London

Olivier Proust
Of Counsel
Privacy, Security & Information Team
Fieldfisher, Brussels

Cecilia Álvarez Rigaudias
Data Protection Officer
Pfizer, Madrid

Bruno Gencarelli
Head of Data Protection Unit
European Commission, Brussels
SESSION OUTLINE

1. GDPR: overview and next steps
2. Rights, obligations & accountability
3. International data transfers
4. A new regulatory approach
5. Getting ready for the GDPR
6. Questions
7. Please give your feedback!
GDPR: OVERVIEW & NEXT STEPS

John Bowman & Bruno Gencarelli
OVERVIEW

- EU Charter of Fundamental Rights sets out that everyone has the right to the protection of personal data concerning them

- The Treaty on the Functioning of the European Union provides that the European Parliament and the Council shall lay down rules relating to the protection of personal data

- Milestones along the path to agreement:
  - January 2012: European Commission publishes proposals for data protection reform
  - October 2013: LIBE Committee vote
  - March 2014: European Parliament first reading
  - June 2015: Council general approach, trilogues commence
  - December 2015: informal compromise agreement following trilogues
**NEXT STEPS IN THE ADOPTION PROCESS**

**Q1-2 2016**
- Lawyer linguist review and translation
- Council vote
- European Parliament vote
- Entry into force 20 days after publication in Official Journal of EU

**Q2-3 2018**
- Rules apply two years after entry into force

**Other activity 2016-2018**
- Agreement of delegated and implementing acts by Commission and Council
- Member state legislation for local carve-outs and law enforcement Directive
- Establishment of EDPB and appointment of chair
- Guidance to be prepared by supervisory authorities
RIGHTS, OBLIGATIONS & ACCOUNTABILITY

Olivier Proust & Cecilia Álvarez Rigaudias
### Key Changes to EU Data Protection Law 1/4

<table>
<thead>
<tr>
<th>Key Issue</th>
<th>Changes introduced by GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Territorial Scope</strong></td>
<td>Broader territorial scope - will apply to: (i) Data controllers <strong>and data processors</strong> established in EU that process personal data; and (ii) Data controllers <strong>and data processors</strong> not based in EU who target individuals who are in the EU</td>
</tr>
<tr>
<td><strong>Data Processors</strong></td>
<td>GDPR introduces direct statutory obligations for data processors, including (i) appointment of a Data Protection Officer; (ii) duty to notify the data controller <strong>without undue delay</strong> in case of a data security breach; and (iii) international data transfer obligations.</td>
</tr>
</tbody>
</table>
| **Expanded definitions / new concepts** | • **Personal Data** - includes location data, online identifiers and technology identifiers  
• **Pseudonymous Data** - defined as data that does not allow identification of individuals without additional information and is kept separate  
• **Sensitive Data** - includes genetic data and biometric data  
• **Profiling** - automated processing of personal data used to evaluate an individual’s “personal aspects”                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Key Issue</th>
<th>Changes introduced by GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent</td>
<td>Consent must be either (i) <em>unambiguous</em> consent for general processing of personal data; or (ii) <em>explicit</em> consent for processing of sensitive personal data.</td>
</tr>
</tbody>
</table>
| Data subject if rights| • Existing rights reinforced (access, rectification, deletion, objection to the processing)  
  • New rights: *erasure* (and right to be forgotten), *restriction* of the processing, data *portability*, right not to be subject to data *profiling* |
| Profiling             | Automated decision making (including profiling) that either produces a *legal effect or significantly affects* individuals must be (i) authorised by law; or (ii) necessary to enter into or perform a contract with that individual; or (iii) based on individual’s *explicit consent*. |
| Minors                | Consent must be obtained from parents when information society services are provided to minors below the *age of 16*.                                                                                                   |
| Enforcement           | DPAs now have *investigative* and *corrective* powers                                                                                                 
  They may impose fines of up to *EUR 20 million* or up to 4% of worldwide annual turnover (whichever is higher)
## Key Changes to EU Data Protection Law 3/4

<table>
<thead>
<tr>
<th>Key Issue</th>
<th>Changes Introduced by GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td>GDPR introduces new explicit principle of accountability - data controllers must ensure compliance with the general data processing principles</td>
</tr>
</tbody>
</table>
| Records of processing activities  | • No more DPA registrations  
• **But** controllers and processors must maintain internal records of all the data processing activities under their responsibility                                                                                                                                                                                                                           |
| Privacy by Design / Privacy by Default | • GDPR introduces new concepts of ‘privacy by design’ and ‘privacy by default’  
• The controller must implement **appropriate technical and organizational measures** which are designed to integrate the necessary safeguards into the processing                                                                                                                                                          |
| Data Protection Impact Assessments | Data controller must carry out a **data protection impact assessment** prior to processing data where the processing is likely to result in a high risk for the rights / freedoms of individuals due to (i) the use of new technologies; (ii) the nature, scope, context and purposes of processing. |

---

#GPS16
## Key Changes to EU Data Protection Law 4/4

<table>
<thead>
<tr>
<th>Key Issue</th>
<th>Changes introduced by GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical and organisational measures</td>
<td>Controllers must implement technical and organizational measures to ensure and be able to demonstrate compliance with the GDPR including the implementation of appropriate policies</td>
</tr>
<tr>
<td>Data breach notification</td>
<td>GDPR introduces an obligation to notify data breaches: (i) to the data protection authority within 72 hours; and (ii) to affected individuals without undue delay.</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>Data controllers and processors must appoint a DPO in case of: (i) regular and systematic processing of data subjects on a large scale; and (ii) when the core activities of the controller or the processor consist of processing on a large scale of sensitive data or data relating to criminal convictions and offences.</td>
</tr>
</tbody>
</table>
INTERNATIONAL DATA TRANSFERS

Olivier Proust & Bruno Gencarelli
DATA TRANSFERS AT A GLANCE

• General principle remains the same: transfers outside the EEA are possible under certain conditions
• Data transfer restrictions apply now both to controllers and processors
• Data transfer rules now apply both to transfers
  – to a third country; or
  – an international organization outside the EEA
• Data transfer rules apply both to initial transfers outside the EEA and onward transfers
LEGAL SOLUTIONS FOR TRANSFERRING DATA

1. Adequacy decision

2. Appropriate safeguards
   • Appropriate safeguards that **do not** require any special authorization from the DPA
     ➢ Standard contractual clauses adopted by the EU Commission
     ➢ Standard contractual clauses adopted by a DPA and approved by the EU Commission **NEW!**
     ➢ Binding Corporate Rules **NEW!**
     ➢ Code of conduct **NEW!**
     ➢ Certification mechanism (e.g., data protection seal or mark) **NEW!**
   • Appropriate safeguards which **do** require specific authorization from the DPA
     ➢ Contractual clauses between the exporter and importer **NEW!**

3. Legal derogations
“Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.” (Chapter V).
A NEW REGULATORY APPROACH

John Bowman & Bruno Gencarelli
SUPERVISORY AUTHORITIES

Tasks of the supervisory authority (selected)

• Promote public awareness of risks, rules, safeguards and rights
• Promote awareness of the Regulation amongst controllers and processors
• Deal with complaints, conduct and co-operate in investigations
• Give advice on processing following a DPIA which indicates a high risk to individuals
• Authorise contractual clauses and binding corporate rules
• Contribute to the activities of the EDPB

Sanctions

• Regarding obligations of the controller and the processor: up to €10 million, or 2% of worldwide annual turnover — whichever is higher
• Regarding the basic principles for processing, data subject rights, transfers of personal data, or noncompliance with an order by the supervisory authority: up to €20 million, or 4% of worldwide annual turnover— whichever is higher
• Other enforcement powers available include issuing warnings and reprimands, ordering compliance with the GDPR, and imposing temporary and definitive bans on processing
ONE-STOP SHOP

• The lead authority is the supervisory authority located in the territory of the main establishment. For matters of cross-border interest, the lead authority will co-ordinate the investigation with other concerned authorities and prepare the draft decision

• If the case is purely a matter that is local to the data subject, the lead authority can delegate competence to deal with the case to the local authority

• If a concerned supervisory authority provides a reasoned objection to a lead authority’s draft decision, the case shall be referred to the European Data Protection Board for a binding decision under the consistency mechanism

• A concerned person may challenge the validity of the implementation of an EDPB decision by a national supervisory authority in a court of the member state where that authority is established

• Any person has the right to bring an action for annulment of decisions of the EDPB before the Court of Justice of the European Union where it is of direct and individual concern to them
GETTING READY FOR THE GDPR

Olivier Proust & Cecilia Álvarez Rigaudias
GDPR COMPLIANCE PROGRAMME

- Business case
- Gap analysis
- GDPR readiness report
- Project plan
STEP 1: BUILD A BUSINESS CASE

• What is your plan?
• Create a brief and easily digestible business case document
• Bring the business case arguments out on the first page
• Focus on key compliance areas in the remainder and show you know what you’re doing
• Slide decks, stakeholder meetings, etc. as required
STEP 2: GAP ANALYSIS

Why, how and who should do it?

1. **Why**: understand where you are against GDPR standards and how much work you have to do

2. **How**: Gap Analysis Questionnaire

3. **Who**: privacy function / DPO leads; senior management backing (**GDPR Champion**); support from legal and compliance; **external counsel**; **project team** to run it; all parts of **business** to input as required.

4. **What’s next**: GDPR Readiness Report
STEP 3: GDPR READINESS REPORT

Sets out for each GDPR compliance area:

1. The GDPR requirement
2. What it means for your company
3. Where your company is now
4. Where it should be to meet GDPR standards
5. How to get there

These are the objectives of your project plan
HOW DID THINGS GO?
(WE REALLY WANT TO KNOW!)

Did you enjoy this session? Is there anyway we could make it better? Let us know by filling out a speaker evaluation.

• Start by opening the IAPP Events mobile app.

• Select this session and tap “Click the following link for speaker evaluations.”

• Once you’ve answered all three questions, tap “Done” and you’re all set.

• Thank you!