Managing Data – Understanding the Impact of the General Data Protection Regulation (“GDPR”)

Ernst Landsberg EY
Shimon Simon EY
Today’s session

- Insights into the background of the regulation and the changes it is bringing.
- Practical lessons on recent engagements undertaken
- How data processing will be impacted and how to operate within the legal requirements.
Why do we need GDPR?

- Dispersed data protection regimes across the European Union
- Different standards applied by national regulatory authorities
- Technological developments form new types of threats for citizen’s privacy
- Protect European citizen’s privacy also outside of the European Union
- Facilitate data flow within the European Union
Why do we need GDPR?

- The volume of **people, process and technology change** required by the 25 May 2018 deadline of the GDPR should not be underestimated.
- Many insurers are compliant, on paper, with existing legislation, but are yet to face the challenge of implementing the requirements through the entire personal data lifecycle.
- As business models have been digitised, the **volume of data** held by organisations has increased significantly, resulting in organisations not understanding how much PI they hold, why they retain it and how it is being used.

**GDPR Timeline**

- **January 2012**: European Commission (EC) proposed GDPR.
- **March 2014**: EU Parliament adopt compromise text.
- **Dec 2015**: GDPR agreed.
- **14 April 2016**: GDPR formally adopted by member states.
- **August 2017**: Release of The exchange and protection of personal data paper.
- **25 May 2018**: GDPR takes effect.
GDPR insights – Key changes snapshot

Key changes

- An (almost) harmonised EU DP regime
- Broad definition of “personal data”
- Extended territorial effect
- Notification regime limited to sensitive data processing / Prior checking approach
- Data protection officer
- One-stop-shop
- International data transfers
- Data minimisation
- Accountability
- Impact assessments
- Privacy by design and by default
- Legitimate interest
- High bar for consent
- Right to be forgotten
- Data portability
- Profiling
- Children
- Clear and plain language
- Transparency
- Penalties for companies
- Security & data breach notification
- Liability of data processor

Scope-Definitions
- Formalities
- New principles
- Appropriate safeguards

Data subjects’ rights
- Legal grounds for data processing

Enforcement / sanctions
- Security and breach notification
## GDPR key changes: Data Protection Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Impact of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fair, lawful and transparent processing</strong></td>
<td>Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. Enhanced compliance burden to document how processing is undertaken lawfully and fairly</td>
</tr>
<tr>
<td><strong>The purpose limitation principle</strong></td>
<td>Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. (Further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes, in accordance with Art.89(1)). Limited to no change for FS clients</td>
</tr>
<tr>
<td><strong>Data minimisation</strong></td>
<td>Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. Replaces “not excessive”. This more restrictive means firms need to carefully consider whether a processing activity is strictly necessary</td>
</tr>
<tr>
<td><strong>Data accuracy</strong></td>
<td>Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay. Limited change as this was previously implicitly required. Failure to do so will though be a data principle breach incurring the higher tier fine</td>
</tr>
</tbody>
</table>
## GDPR key changes: Data Protection Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Impact of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data retention</strong>&lt;br&gt;Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, historical, or statistical purposes in accordance with Art. 89(1) and subject to the implementation of appropriate safeguards.&lt;br&gt;</td>
<td>Limited to no change for FS clients.</td>
</tr>
<tr>
<td><strong>Data security</strong>&lt;br&gt;Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.&lt;br&gt;</td>
<td>What was a previous Directive requirement is now a data protection principle. Information Security should now be seen as a fundamental obligation</td>
</tr>
<tr>
<td><strong>Accountability</strong>&lt;br&gt;The controller is responsible for, <em>and must be able to demonstrate</em>, compliance with the Data Protection Principles.&lt;br&gt;</td>
<td>Demonstrable compliance now required</td>
</tr>
</tbody>
</table>
### GDPR key changes (1/2)

<table>
<thead>
<tr>
<th>Expanded scope</th>
<th>Applies to all data controllers and processors established in the EU and organizations that target EU citizens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent</td>
<td>▶ Consent must be provided by an and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her</td>
</tr>
</tbody>
</table>
| 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 Impact Assessments | Organizations must undertake Privacy Impact Assessments when conducting risky or large scale processing of personal data |
| Privacy by Design | Organizations should design data protection into the development of business processes and new systems |
### GDPR key changes (2/2)

<table>
<thead>
<tr>
<th>Data Protection Officers (DPOs)</th>
<th>DPOs must be appointed if an organization conducts large scale systematic monitoring or processes large amounts of sensitive personal data</th>
</tr>
</thead>
</table>
| Accountability                   | Organization 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 |
| Obligations on processors        | New obligations on data processors — processors become an officially regulated entity |
| 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, those individuals must be informed as well |
| 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, whichever is greater |
GDPR: 14 Capabilities

- Data Privacy Accountabilities
- Privacy Impact Assessment
- Personal Data Flow Mapping
- Governance
- Data Privacy Risk & Control Framework
- Incidents
- Third Party Oversight
- Conditions for Processing
- Use of personal data
- Security
- Data Privacy Notifications
- Consent
- Retention & Individuals rights
- Complaints & Compensation
- Data subject access requests
- Data subject rights
- Data portability
- Data subject rights
GDPR: 14 Capabilities by Implementation Difficulty

### Governance
1. Data Privacy Accountabilities
   - Responsibilities documented and articulated.
2. Privacy Impact Assessment
   - Form of PIAs is defined and agreed. Use of PIA in business agreed and use is started.
3. Personal Data Flow Mapping
   - DFM are in progress and understood. PIAs are interlinked and used as appropriate.
4. Data Privacy Risk & Control Framework
   - Demonstrable compliance to the GDPR is in place. Clear framework of controls including DPO.
5. Incidents
   - Data breaches are recognised quickly, full extent of processing activities is known.

### Compliance
6. Conditions for Processing
   - Legal basis for processing client and colleague data understood and demonstrable.
7. Consent
   - Use of data fully understood. Explicit consent captured where necessary.
8. Data Privacy Notifications
   - Use of data is fully known (i.e. marketing), this is reflected and communicated in clear DPNs.
9. Security
   - Personal data is held securely. Potential use of encryption and standards followed.
10. Third Party Oversight
    - Third parties network known. Contractual elements in place for compliance.

### Individual Rights
11. Retention & Individuals Rights
    - Able to effectively facilitate new rights e.g. erasure, rectification etc.
12. Data Subject Access Requests (DSARs)
    - Raise in requests anticipated, planned and mechanisms in place to facilitate.
13. Data Portability
    - Portability considered and enabled (in line with PSD2). Applications for products and services.
14. Complaints and Compensation
    - Data subject complaints processed effectively and consistently.
Client challenges

- Setting budget and resource allocation to GDPR programmes
- Records of processing: Mapping through legacy IT systems and processes
- Lack of industry consensus on approach to data portability
- “Right to be forgotten” versus other regulatory and legal obligations

- Linkage between the GDPR programmes and BAU activities
- Dependency management — within programmes and within the business
- Setting a clear vision and defining compliance for the organisation
- Identifying the home for Data Protection and the new DPO role within the organisation

- Data - the use of profiling within marketing activities customer profiling
- Opt in vs. Opt out — historical and future approach to consent
- Setting programme scope for GDPR and limiting scope creep
- Managing communications and creating a ‘culture of data protection’
Question & Answer – General

From a UK perspective, how different is GDPR from existing data protection requirements?

How is GDPR training being done in firms?

How are communications with customers changing as a result?

I keep hearing the expression “consent journey” - please can you explain what is meant by this?

What does “right to be forgotten really mean?”

Can we trust the Information Commissioner’s Office (ICO) when it says that 100% compliance is not needed on May 2018 as long as material areas addressed, roadmap to full compliance laid out and resources allocated?

Surely the ICO will be gunning for Amazon and Google. Do they care about insurance companies?

What about policies that were incepted before more modern consent journeys?

What do you expect the ICO focus to be around insurance companies?
An Actuarial valuation does not normally have a person’s name, NI number, but sometimes you get detail on postcode, sex, DOB etc. and one could identify the person - is that a problem?

What about the Group policies - assume consent is required for all individuals?

What about process of health data and consent for use for GP reports?

Obviously for U/W purposes, Actuaries collect lots of personal data with consent - assume this is OK and they carry on? What about joint life cases?

We can start getting consent for new business, but what do we need to do about our existing customer base?
Clearly we can do experience analysis as before? But careful where extracts include personally identifiable data e.g. postcode, age, N.I.

Life companies often use outsourced providers - assume they will need to get p/h consent to share data with these firms?

Big issue is Actuaries like to store data on their own data stores and I assume this is a potential GDPR problem? What are the implications for them?
Review how data shared between insurers and reinsurers will need consent or the data is anonymised?
The views expressed in this presentation are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this presentation and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this presentation.

The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this presentation be reproduced without the written permission of the authors.