Introduction to GDPR for Law Firms

Presented by
Ed McNicholas
Patrick Won, JD

Moderator
Rick Hellers

OM36
5/5/18
3:00 PM
Introduction to GDPR for Law Firms

ALA Annual Conference
May 5, 2018

Rick Hellers, Association of Legal Technologists
Ed McNicholas, Sidley
Patrick Won, Integreon

Faculty

Rick Hellers
Founder of Association of Legal Technologists

Edward McNicholas
Co-Leader with Sidley’s Privacy and Cybersecurity practice

Patrick Won
Manager of Contracts, Compliance and Commercial Services at Integreon.
Today’s Agenda
1. GDPR Basics
2. Problems for Law Firms
3. Building a Compliant Program
4. Contract Issues
5. Questions & Answers

Why is data important?

A few numbers:

65% of boards rarely or never review their key information, data assets and personal data to confirm legal, ethical and security implications

4% fines of 4% of annual worldwide turnover under the new EU General Data Protection Regulation

169 over 169 million records were exposed in 2015, stemming from 781 publicized breaches

38% in 2015, there were 38% more security incidents detected than in 2014

77% of businesses are now allocating budget to protect consumer data

16% only 16% of boards have a clear understanding of their data assets

€1 the value of European citizens’ personal data could grow to nearly €1 trillion annually by 2020

16% only 16% of boards have a clear understanding of their data assets

50% half of all European Internet users are worried about becoming a victim of fraud through the misuse of their personal data

270$ by 2020 the cloud computing market will be worth $270 billion

SIDLEY AUSTIN LLP
GDPR – who does it impact?

Wide scope and extra territorial affect

**Data controllers and data processors**
- A **data controller** determines the purposes and means of the processing of personal data.
- A **data processor** processes personal data on behalf of a data controller.
- The GDPR will directly impose obligations on data controllers AND processors.

**Extra territorial affect**
- The GDPR will apply to almost all companies established in the EU. The GDPR will also apply to companies processing the personal data of EU-based individuals, even where they are not established in the EU if they are offering individual in the EU goods or services or monitoring them.

**All industries affected**
- Tech companies, life sciences, financial services, retail etc.
- Multinational companies and small businesses

**All types of personal data**
- Employee data
- Customer data
- End user data
- Vendor data

Impact of the GDPR

Implementation and violation

- GDPR adopted in 2016 and will come into force in **2018**
- Increase in privacy litigation by customers
- GDPR applies to businesses in the EU and any company **worldwide** that holds data on Europeans
- Damages will now be permitted for non-financial loss e.g., for distress
- Fines of up to 4% of annual **worldwide** turnover or €20m, whichever is greater
- Claims by individuals or representative organisations
GDPR - Key Terminology

What does it mean?

- **Processing**: is the collection, use and destruction of personal data.
- **Data subject**: is the individual about whom the personal data relates.
- **Personal data**: (i.e., any data which can help identify a living person) – it includes data, which by itself does not identify a person but when added to other data, does identify a person e.g. a payroll number can be linked to an individual by inputting it into systems.
- **Sensitive personal data**: are data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

GDPR Problems for Law Firms
A New Data Privacy Regime

Opportunities under the GDPR

**Opportunities**

- Increased trust between individuals (e.g. customers) and businesses
- Potential for increased engagement (i.e. through the decrease in usage of ad blockers and tracking)
- Protection of reputation
- Standardisation of processes across the EU

Challenges under the GDPR

**Challenges**

- Organisations have greater responsibility for how they handle data
- It entails a number of new, onerous obligations, the implementation of which will require structural changes for business
- There will be compliance costs attached to implementation (e.g. cost of amending contracts to be GDPR compliant, amending privacy policies and notices and amending procedures to deal with data subject rights)
### Building a GDPR Compliance Program

**Data Protection Principles**

**7 Principles**

<table>
<thead>
<tr>
<th>Principles</th>
<th>Actions to comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Fair and lawful processing</td>
<td>• Employee, customer and end-user notices need to contain certain information as set out in the GDPR</td>
</tr>
<tr>
<td></td>
<td>• Establish a legal ground for the processing (e.g. legitimate interest of the business)</td>
</tr>
<tr>
<td>2. Purpose limitation</td>
<td>• Be clear from outset why you are collecting data and what you intend to do with it</td>
</tr>
<tr>
<td></td>
<td>• Avoid “function creep” – only use data for reasons given</td>
</tr>
<tr>
<td>3. Data Minimization</td>
<td>• Specify purposes in a privacy notice to data subjects</td>
</tr>
<tr>
<td></td>
<td>• Do not collect / hold more information than you need for the particular purpose</td>
</tr>
<tr>
<td></td>
<td>• Do not hold personal data on the off-chance that it might be useful in the future</td>
</tr>
</tbody>
</table>
### Data Protection Principles

#### 7 Principles

<table>
<thead>
<tr>
<th>Principles</th>
<th>Actions to comply</th>
</tr>
</thead>
</table>
| **4. Accuracy** – personal data shall be accurate and, where necessary, kept up to date | - Take reasonable steps to ensure the accuracy of any personal data you process  
- Consider whether it is necessary to update the information |
| **5. Storage Limitation** – personal data should not be kept for longer than is necessary for the relevant purpose | - Review the length of time you keep personal data  
- Data Retention Policy?  
- Update, archive / delete personal data if you no longer need it for the specific purpose |
| **6. Security** – implement appropriate technical and organisational measures to protect personal data (to be discussed later) |  |

---

### Data Protection Principles

#### 7 Principles

<table>
<thead>
<tr>
<th>Principles</th>
<th>Actions to comply</th>
</tr>
</thead>
</table>
| **7. Accountability** – a requirement to demonstrate compliance with Principles 1-6 and the requirements under the GDPR more generally | - Privacy impact assessments must be carried out where data processing uses new technologies and results in high risk to individuals  
- Privacy by design and by default - implement technical and organisational measures to ensure privacy (e.g., encryption) AND by default only the minimum amount of personal data are processed  
- Detailed record of processing activities must be maintained and provided to DPA upon request  
- In certain cases a business must appoint a data protection officer |

**SIDLEY AUSTIN LLP**
### Data Subject Rights

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Actions to comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to erasure – a business must erase an individual's personal data in certain circumstances</td>
<td>If you receive a request from a data subject you should contact the [Legal Department]</td>
</tr>
<tr>
<td>Right to data portability – individuals have right to request the transfer of their personal data from one company to another in certain circumstances</td>
<td>Act quickly as a response must be given within 1 month</td>
</tr>
<tr>
<td>Right to object – individuals have right to object to processing of their personal data and to direct marketing</td>
<td></td>
</tr>
<tr>
<td>Right of access – individuals have a right to access and obtain copies of their personal data</td>
<td></td>
</tr>
<tr>
<td>Right to rectification – Individuals have right to have their personal data rectified if it is inaccurate or incomplete</td>
<td></td>
</tr>
<tr>
<td>Right to restrict processing – individuals have right to restrict processing of their personal data</td>
<td></td>
</tr>
</tbody>
</table>

### Profiling

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Actions to comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiling – individuals have the right not to be subject to decisions made automatically that produce legal effects or significantly affect the individual. This right does not apply where the decision is: • based on explicit consent from the individual; • necessary for a contract with the individual; or • authorized by EU or Member State law</td>
<td>Review and amend current profiling activities, where appropriate</td>
</tr>
<tr>
<td></td>
<td>If profiling activities fall within scope of restrictions: • Can you rely on one of the exemptions? • If no, amend profiling activities</td>
</tr>
</tbody>
</table>

**SIDLEY AUSTIN LLP**
## Information Security

### Information security, breach reporting and vendors

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Actions to comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk</td>
<td>Review and comply with (i) information security standards; and (ii) data breach response plan and reporting procedures</td>
</tr>
<tr>
<td>Security breaches must be reported to: (i) the DPA without undue delay and where feasible within 72 hours; and (ii) affected individuals without undue delay where high risk, unless measures taken to minimise risk, e.g., the data is encrypted</td>
<td>Conduct a review of key vendor agreements to ensure they include GDPR-compliant data processing provisions</td>
</tr>
<tr>
<td>Data Processors – Company is responsible for ensuring processors (e.g. vendors) comply with security and processing measures</td>
<td>Conduct data protection due diligence on key vendors</td>
</tr>
</tbody>
</table>

SIDLEY AUSTIN LLP

---

## International Transfers

### Requirements

- **Prohibition** on transfers of personal data outside EEA to countries that do not provide adequate safeguards (e.g., U.S.)

### Actions to comply

- Before sharing personal data, determine any international data flows and implement a data transfer solution

### Data transfer solutions are exceptions to the prohibition on international data transfers and include:

- the new EU-US Privacy Shield which applies to transfers of personal data to US companies that are Privacy Shield certified
- EU Standard Contractual Clauses which are EU style data transfer agreements but which are under review by EU Authorities
- Binding Corporate Rules which is a set of privacy rules adopted by a group of companies and which comply with strict EU standards
- approved Codes of Conduct or Certification Mechanisms

SIDLEY AUSTIN LLP
GDPR Contract Issues

With deadlines looming, ALSPs can help solve GDPR compliance challenges with:

- Review of Existing Policies and Procedures and Gap Analysis
- Review and Summarize Contracts, including Notice and Amendment Provisions
- Drafting Notice Amendment Template(s)
- GDPR Contracting Playbook Drafting and Escalation Process Design
- Issue and Negotiate Notice Letters and Amendments
- Structured Data Entry and Management of Amendments
GDPR Compliance – Deeper Dive

**Fines up to 4% of Global Turnover**
Regulators can impose a fine of up to 4% of Global turnover or €20,000,000, whichever is greater.

**Expanded Scope**
Applies to all data controllers and processors in the EU as well as 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**
Organizations must prove they are accountable by:
- Establishing a culture of monitoring, reviewing and assessing data processing procedures
- Minimizing data processing and retention of data

**Privacy Data Impact Assessment**
Organizations must undertake Privacy Impact Assessments when conducting risky or large scale processing of personal data.

**Consent**
- Consent must be "explicit" in the case of sensitive personal information or transborder information flow
- Customers must be informed of their right to withdraw their consent
- Consumer consent to process data must be freely given and for specific purposes

**Mandatory Breach Notifications**
Organizations must notify regulators of data breaches "without undue delay" or within 72 hours, unless the breach is unlikely to be a risk to individuals.

**Obligations on Processors**
New obligations on data processors – processors become regulated entities.

---

Contract Issues – Review, Analysis and Development

<table>
<thead>
<tr>
<th>Today</th>
<th>May 2018 and beyond</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client</strong></td>
<td>GDPR/Program Management</td>
</tr>
<tr>
<td><strong>Consulting Firms</strong></td>
<td>Operational &amp; Technology Workstreams and Consulting</td>
</tr>
<tr>
<td><strong>Outside Counsel</strong></td>
<td>Legal Advisory</td>
</tr>
<tr>
<td><strong>ALSP Support</strong></td>
<td>Review Existing Policies &amp; Procedure, Perform Gap Analysis – 2 Phase Approach</td>
</tr>
</tbody>
</table>

**Phase 1: Review & Analysis**
- Review of Corp. Data Policy / Protection Procedures
- Gap Analysis

**Phase 2: Development**
- Develop GDPR Compliance Rating Methodology
- Develop GDPR Risk Management Plan
Introduction to GDPR for Law Firms

ALA Annual Conference
May 5, 2018

Rick Hellers, Association of Legal Technologists
Ed McNicholas, Sidley
Patrick Won, Integreon
Your opinion matters!

Please take a moment now to complete the evaluation.

Thank You!