General Data Protection Regulation (GDPR)

Software & Information Industry Association (SIIA)
Carl Schonander/Senior Director, International Public Policy
cschonander@siia.net
Tel: 202 – 789 - 4456
Goals for This Presentation

- Give a sense for what the EU is trying to achieve with the GDPR
- Provide additional information and resources
- Identify the key topics for software and digital media companies
History

- European Commission proposed GDPR on 1/25/12 as a revision of the 1995 Directive.
- Final text of the GDPR was published on April 6, 2016.
- This DSB-MIT-SYSTEM presentation has a table of contents and easy to use hyperlinks to individual articles and recitals.
- The GDPR was published in the EU’s Official Journal on May 4, 2016.
- The legislation goes into effect on May 25, 2018.
What Are The Key Changes?

This European Commission document explains succinctly why companies need to care

• Increased territorial scope (Article 3); office in the EU is not needed for GDPR to apply
• Penalties (Article 84) – up to 4% of global turnover
• Consent (Articles 7-8) – consent docs have to be written clearly, i.e. not in “legalese”
• Breach notification (Article 34) – 72 hour breach notification requirement
• Right to access (Article 15) – customers have a right to access their data
• Right to be Forgotten (Article 17) – applies basically to search
• Data Portability (Article 20) – consumers have a right to their data in a machine-readable format
• Privacy by Design (Article 25) – privacy expected to be built in for new processing
• Data Protection Officers (Article 37-39) – firms subject to GDPR will need them
Who Does the GDPR Apply to?

• Article 3 (page 110) on Territorial scope applies
  1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
  2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
     (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
     (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
  3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.
What Is Personal Data?

• See article 4
• For the purposes of this Regulation:
  • (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
And Who is Covered under GDPR?

• Even if you do not have an office in an EU country, if you offer services (even if not for payment) to EU citizens “in the Union,” you are subject to the GDPR

• If you offer services to EU citizens outside the Union, you are not subject to the GDPR
How To Prepare?

• See the British Information Commission on what to expect in the run-up to entry-into-force
• See the British Information Commission Getting Ready for the GDPR SME Toolkit
• And 12 steps to take now (see page two especially)
• Note: UK to join GDPR despite Brexit
Awareness

• Make sure management knows about GDPR, why it matters to the company, and what the company needs to do to comply
• Management should care if for no other reason than that potential fines can reach 4% of global turnover
• Data Protection Authorities (DPAs) will be on the lookout for issues so reputation risk should also be considered
Information Held

- Document what personal data is held, where it comes from and with whom it is shared, and consider undertaking an information audit
Communicating Privacy Information

• Review current privacy notices and formulate a plan for making any necessary changes before the GDPR takes effect.
Individuals’ Rights

• Review procedures to meet rights –Chapter III, 129-149
• Article 15 right of access
• Article 16 right to rectification
• Article 17 right to erasure or right to be forgotten
• Article 18 right to restriction of processing
• Article 20 right to data portability
• Article 21 to object and automated processing
Subject Access Requests

• Update procedures to ensure organizations address all of the rights that individuals will have under the GDPR.
Legal Basis for Processing

• Review data processing activities and identify and document the legal basis for each type of data processing activity
• See Article VI
• Consent the default rule but “legitimate interests” still possible
Consent

• Review how the organization seeks, obtains, and records consent, and consider whether any changes are needed.
Children

• Consider implementing new systems to verify individuals’ ages and to gather, where relevant, parental or guardian consent for the data processing activity.
Data Breaches

• Make sure appropriate procedures are in place to detect, report, and investigate data breaches

• See Article 33
  • Article 33 Notification of a personal data breach to the supervisory authority
  • 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
Data Breaches Continued

• Article 34 deals with obligations towards data subjects
• Article 34 Communication of a personal data breach to the data subject
  • 1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
Data Protection by Design and Data Protection Impact Assessments (DPIAs)

• Become familiar with ICO guidance on Privacy Impact Assessments and determine how and when they should be implemented.
DPO

- Designate a Data Protection Officer (DPO), if required, or someone to take responsibility for data protection compliance. Determine where the role will sit within the organization’s structure and governance arrangements.
International

• If the organization operates internationally, determine what mechanism you use to transfer data from the EU to another jurisdiction, e.g. the United States

• Options include the EU-US Privacy Shield, Binding Corporate Rules, and Model Contracts
Bavarian Data Protection Authority Questionnaire

- You can find the questionnaire in English here.

- This might be the single most useful document currently available for GDPR preparation because it provides an easy to understand checklist of things to do.

- The questionnaire has already been sent to 150 randomly selected companies, although they are not obliged to respond.
There are questions pertaining to:

- Structure and responsibility in the company (e.g. is there a data protection officer?)
- Overview of processing activities (e.g. are there records and privacy by design?)
- Involvement of third parties (e.g. do you have the right contracts with processors?)
- Transparency, information duties and assurance of data subject rights (e.g. what is the legal basis for processing – if “legitimate interest,” specify what it is)
- Accountability, risk management (e.g. can you demonstrate that consent has been given?)
- Data breaches (e.g. have you ensured you can notify within 72 hours?)
Commission/DPAs Working on Guidance

• Article 29 Working Party has issued guidance on data portability, data protection officers, lead supervisory authority, data processing at work, data protection impact assessments (DPIAs) and when they are needed

• Working Party plans to release guidance on profiling and automated decision making in October and by the end of the year there will be guidelines on consent, transparency and breach notification
Data Portability (the right or ability to transfer data from one controller to another) and SIIA

- SIIA submitted comments in response to the Article 29 Working Party – we argue that:
  - The data portability right does not always make economic sense.
  - The portability right arises in business to consumer relationships.
  - Data processors should not be liable for the portability obligations of their controller customers
  - Only data that is affirmatively provided by the data subject should be covered by the right.
  - There should be no requirement for uniform data formats.
  - APIs are good but companies should not be obliged to develop them.
  - There should be no obligation to re-identify pseudonymous data.
So, What Should You Do?

- Determine whether you are subject to GDPR. You probably are!
- Decide whether to appoint a DPO – you probably should. You don’t have to necessarily create a new headcount to do this but the designee has to be somebody who can logically fill the role.
- Make sure your consent language is easily understandable. If consent is not the basis for your processing, understand what legal basis you have for the processing.
- Review contracts with processors.
- Determine whether you handle particularly sensitive data – if you do you might have to do a Data Protection Impact Assessment (DPIA) for new operations. “Sensitive data” often involves processing that could have a legal effect on a data subject.
- Make sure you understand on what legal basis you process data if it is not consent.
- Make sure you can explain to a DPA how you can fulfill data subject rights.
- Determine what mechanism to use if you transfer data outside the EU (Privacy Shield, Binding Corporate Rules or Model Contracts).
Questions
The End