GDPR is Coming – Are You Ready?

Presented by Robert J. Scott

The Association of
CAUCUS
Technology Acquisition Professionals

Agenda

- GDPR Key Changes
- Purpose
- Applicability
- New Rights
- Enforcement
- Data Breach
- Roadmap/Decision Tree
- Preparation

GDPR Key Changes

Examples:

- Regulation
- Broader Scope & Definitions
- Data Protection Officer (DPO)
- Data Protection Risk Assessment (DPIA)
- Data Breach Notification Requirements
- Data Transfer / Data Portability
- Privacy by Design / Privacy by Default
- Greater Penalties

Purpose

- The processing of personal data is a fundamental right, which needs protection.
- Imposes specific obligations on “Processors”, “Controllers”, and others with regard to their vendor relationships and the protection of “Personal Data”.
- Requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

Applicability
Subject Matter & Objectives

- Lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. (Art. 1(1))
- Protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. (Art. 1(2))
- Free movement of personal data within the EU shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. (Art. 1(3))

Applicability
Scope

- **Material**
  - Personal data is processed in connection with the goods or services to EU citizens, irrespective of payment. (Art. 3(2)(a))
  - EU data subjects' behavior is monitored. (Art. 3(2)(b))

- **Territorial**
  - EU Organizations – organizations established in the EU (Art. 3(1))
  - Non-EU Organizations – organizations that process data about people in the EU (Art. 3(1))
  - International data transfers –transference of data outside the EU or EEA

New Rights

- Right to rectification (Art. 16)
- Right to be Forgotten
- Right to restriction of processing (Art. 18)
- Right to Data Portability (Art. 20)
- Right to Object (Art. 21)
- Privacy by Design (Art. 25)
- Privacy by Default (Art. 25)
- Consent

Enforcement

- **Supervisory Authority (“SA”)** – Independent public authority from each Member State in the EU with the authority to regulate compliance with GDPR.
- **Data Protection Authority** - Independent public authority responsible for monitoring the application of data protection law within its territory.
- **European Data Protection Board (“EDPB”)** - Has the status of an EU body with legal personality and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification.

Enforcement

- **Fines**
  - Up to 10M EUR or 2% of organization's prior year's worldwide turnover. (Art. 83(4))
  - Up to 20M EUR or 4% of organization's prior year's worldwide turnover. (Art. 83(5))
- **Private Right of Action**
  - Extended to actions against data processors for breaches of the applicable sections of GDPR.
  - Burden of proof lies with the data controller and/or processor. (Art. 79, Art. 82)

Data Breach

- **Definition –** “A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

- **Notification Requirements -** 72 hour notification to the relevant supervisory authority (Main Establishment). If notification is not made within 72 hours, the controller must provide a “reasoned justification” for the delay.

Roadmap & Decision Tree

Steps to ascertain whether a business is required to be compliant with GDPR:

- **Territorial Scope**
  - Is your business located in the EU? (Art. 3(1))
  - Are you offering goods or services in the EU, regardless of whether payment is required? (Art. 3(2)(a)
  - Are you monitoring the behavior of EU data subjects, as far as their behavior takes place in the EU? (Art. 3(2)(b))

Roadmap & Decision Tree

- **Personal Data**
  - Is the personal data" in possession 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? (Art. 4(1))

Roadmap & Decision Tree

- **Personal Data**
  - Are you processing personal data of EU data subjects?
    - ”Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Use Case Chart – Service Offerings

SCOTT TECHNOLOGY ATTORNEYS

General Data Protection Regulation ("GDPR") - Controllers

Definitions

- **"Controller"** means "the person or entity that determines, alone or jointly with others, the purposes and the means of the processing of personal data." (Art. 4(7))
  - This definition has three characteristics: (1) separate legal personality, (2) the ability to act alone or with others, and (3) a degree of control over the data processing activity.
- **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, **retrieval***, consultation, **use****, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
  - ***"Retrieval"** is not defined under GDPR. However, "record retrieval" is generally defined as "This term refers to the process of location a specific file, document or record and then delivering it so it can be used." (See Black's Law Dictionary)
  - ****"Use"** is not defined under GDPR. However, "use" is generally defined as "the right to enjoy the benefits of property, whether the owner of the right has ownership of title or not." (See Black's Law Dictionary).
  - **Note**: "Access" is not defined under GDPR. However, "systems access" is generally defined in terms of "Authority or ability to interact with a computer system that results in flow of information; way to input or output data from a sauce of information. Access implies authorization" (See Black's Law Dictionary)

General business activities related to processing:

- Collecting Personal Data
- Recording Personal Data
- Organizing Personal Data
- Structuring Personal Data
- Storing Personal Data
- Adapting or Altering Personal Data
- Retrieving Personal Data
- Consulting with Personal Data
- Use of Personal Data
- Disclosure by Transmission of Personal Data
- Dissemination or making Personal Data available
- Alignment or Combining Personal Data
- Restricting Personal Data
- Erasing or Destroying Personal Data

Types of personal data commonly processed or used by controllers in day-to-day business operations:

- **Customer**
  - Personal information about Customers that could be attributed to B2C oriented businesses. Examples could include the personal details about the owner of a Bank account or a Loan
- **Client**
  - Personal information about a Client that could be attributed to B2B oriented businesses. Although this definition is often associated with the name of a business, many businesses have the owner's name as part of the company name. An example could include 'Andrew Joss Consulting' which, although is a fictional company, might include the actual name of the owner in the title
- **Policyholder**
  - Personal information about an Insurance Policyholder for a wide range of potential products or services. Based upon the above two definitions, this could be related to either B2C or B2B oriented businesses
- **Beneficiary**
  - Personal information that isn't about a defined 'Customer' or 'Policyholder' but personal data about somebody attached or identified against a specific Financial Services product. An example could be an identified spouse to receive a survivors' pension after the death of a 'Policyholder'
- **Contact**
  - Personal information often associated with a Client (in the B2B world) which, although not specifically the company in question, identifies individuals who might be used as contact points within that company and could be seen as individuals associated to a company
  - This definition can also be used for data collected about individuals or groups that are prospects of an organization
- **Employee**
  - Personal information on employees within an organization. Given the potential business structure to many modern businesses, the definition of what an 'employee' is could vary considerably
- **Contractor**
  - Personal information on individuals or businesses that have a contract of some form. This could include agency or temporary staff
- **Volunteer**
  - Personal information on individuals or groups that provide products or services where they are neither classed as employees or on contract. This group may not feature in an HR or contract system and therefore could be outside any data management environment
- **Visitor**
  - Personal information on individuals or groups that may have no formal linkage to the organization but whose privacy data may be collected. An example could include a visitor from a third party organization to the institution
- **'Other'**
  - This is a catch-all definition for personal data that may get collected as part of any business process and that doesn't fit in any previous category.

Use Case Chart – Service Offerings

Use Case Chart												
Business Activities – Examples of different types of "personal data"	Business located in EU Data contains EU data subject "personal data" Services offered must be GDPR compliant				Business not located in EU Data contains EU data subject "personal data" Services offered may / may not need to be GDPR compliant				Business not located in EU Data does not contain EU subject Services offered do not need to be GDPR compliant			
	Good or Services not offered in the EU	Good or Services offered in the EU	Processing data	Monitoring data	Good or Services not offered in the EU	Good or Services offered in the EU	Processing data	Monitoring data	Good or Services not offered in the EU	Good or Services offered in the EU	Processing data	Monitoring data
• Employee data o Name, job title, birth date, passport data, private address, private telephone number, private email address, emergency contact, employee number, status (active or not), birth date, department ID, name of department, supervisor ID, name of supervisor, work location, days of absence and cause, holiday entitlement o Education details, CV, work history with the firm, working hours (full or flex time) o Performance data, compensation data, payroll data, bank account data o Credit card data, transaction data from credit cards, o Frequent flyer program data, travelling preferences	✓	✓	✓	✓	✓	✓	✓	✓	x	x	x	x

Roadmap & Decision Tree

- **Types of entities under GDPR**
  - Are you a “controller”, “processor”, or “sub-processor” of personal data regarding EU data subjects? (Art. 4(2))
    - Controller – determines purpose and means of processing personal data
    - Processor – processes personal data on behalf of controller
    - Sub-processor – processes personal data on behalf of the processor with controller consent

Roadmap & Decision Tree

- **Legal Requirements for Compliance for Controllers**
  - Contract/Transactional Compliance:
    - Contract updates & GDPR addendum
    - Security policies
    - Privacy policies
    - Consent
    - DPO appointment
    - NDA/Confidentiality Agreements
    - Insurance

Roadmap & Decision Tree

- **Legal Requirements for Compliance for Controllers**
  - Processing Compliance
    - Processing Principles
    - Lawfulness of Processing
    - Conditions for Consent
    - Data Security
    - Liability – Joint Controllers
    - Appointment – Representatives / Processors
    - Cooperation
    - Data Breach Notification
    - Certification

GDPR Preparation Cheat Sheet

1. Ensure key stakeholders are aware of the GDPR
2. Identify the information you hold
3. Review current privacy notices and make necessary changes
4. Review procedures for deletion of personal data and availability via commonly used format
5. Review procedures on how to handle data subject access requests
6. Identify lawful basis for processing activity and document in privacy notices
7. Review how you seek, record, and manage consent and update any existing consent processes
8. Review process for identifying individual ages and obtaining parental/guardian consent for processing activities
9. Ensure right procedures are in place to detect, report, and investigate a personal data breach
10. Review Data Protection by Design and Data Protection Impact Assessment guidance (Article 29) and decide when to implement
11. Designate individual to take responsibility for data protection compliance and assess where in the organization the role belongs
12. Determine your lead data protection supervisory authority, if your organization operates in more than one EU member state

Notable Articles

- **Article 5:** Managing access to data / protecting from unauthorized access
- **Article 25:** Data privacy by design, including the use of pseudonymization
- **Article 32:** Implement appropriate technical measures, including encryption; Assess the effectiveness of security measures
- **Article 34**: In the event of a breach, the controller must notify affected data subjects - unless encryption was in place at the time of breach

Be Prepared

- GDPR enforcement will begin around **May 25, 2018**.
- GDPR requires significant changes for organizations who monitor or process EU citizen's personal data.
- Time is much shorter than it seems to get the above mentioned items implemented. If you have not done so already, seek legal counsel.

IT PROCUREMENT ACADEMY

Questions?

Association of CAUCUS Technology Acquisition Professionals

Contact Information

Robert J. Scott, Esq.
Managing Partner
rjscott@scottandscottllp.com
(214) 999-2902

Scott & Scott, LLP.
1256 Main Street, Suite 200
Southlake, TX 76092
www.scottandscottllp.com