THE GENERAL DATA PROTECTION REGULATION ("GDPR")

Tsutomu L. Johnson

November 7, 2016

Salt Lake City

PARSONS BEHLE & LATIMER

History

- Before we get into the GDPR, we have to understand the European Data Protection Directive.
  - Leveraging the fundamental freedom of privacy in Europe, the Directive established the following:
    - Controller and Processor relationships;
    - Broadly defined the terms Personal Data and Processing;
    - Created contractual obligations for suppliers and vendors to preserve privacy;
    - Created a framework for multinational organizations to process information within the organization; and
    - Created the first data localization rules.

PARSONS BEHLE & LATIMER

GDPR at a Glance

- The GDPR is organized s follows:
  - General Provisions (Art. 1-4)
  - Privacy Principles (Art. 5-11)
  - Data Subjects' Rights (Art. 12-23)
  - Controller and Processor Obligations (Art. 24-43)
  - International Data Transfers (Art. 44-50)
  - Remedies, Liability, and Penalties (Art. 77-84)

PARSONS BEHLE & LATIMER

General Provisions

- Definitions:
  - Personal Data: ANY information that can be used to directly or indirectly identify a natural person.
  - Processing: Any operation or set of operations performed on Personal Data whether by automated means or not.
  - Controller: The entity or person which alone, or with others, determines the purposes and means of the Processing Personal data.
  - Processor: An entity or person which Processes Personal Data on behalf of a Controller.
  - Profiling: Any type of automated processing to evaluate a natural person for things like a person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
  - Pseudonymization: Processing Personal Data in such a way that it can no longer be attributed to a specific person without the use of additional information which is protected by an organization's technical and organizational measures. Example: encryption.

PARSONS BEHLE & LATIMER

General Provisions

- Territorial Scope:
  - The GDPR applies to:
    - Controllers and Processors not established in the EU that Process,
    - Personal Data belonging to people in the EU,
    - where activities are related to:
      - Offering goods or services, irrespective of whether a payment is required; or
      - Monitoring of behavior as far as that behavior takes place in the EU.

PARSONS BEHLE & LATIMER

Privacy Principles

- Processing Personal Data
  - Personal Data must be Processed lawfully, fairly, and transparently.
  - Controllers can only collect Personal Data:
    - For a specific, explicit, and legitimate purpose and cannot Process Personal Data in a manner incompatible with that purpose.
    - Where it is adequate, relevant, and limited to what is necessary in relation to the purpose it was gathered.
    - If the Personal Data is accurate.
    - If kept in a form permitting identification of people for no longer than is necessary for the purpose the Personal Data was initially gathered.
    - If it is Processed in a manner that ensures appropriate security and protection against unauthorized use or unlawful Processing.

PARSONS BEHLE & LATIMER

Privacy Principles

- Lawfulness of Processing: The following are the limited situations where it is lawful to Process Personal Data:
  - If a person gives consent.
    - If Processing is based on consent, the Controller must demonstrate that a person has freely given consent that is specific and informed. The consent must demonstrate clear affirmative agreement to Process Personal Data.
    - Note: a person can withdraw consent at any time and force a Controller to stop Processing the person's Personal Data.
  - For a contract wherein the EU resident is a party to the contract or is about to enter into a contract with the Controller.
  - Legal compliance.
  - Protecting a person's vital interests.
  - For Processing carried out in the public's interest.
  - For the Controller's legitimate interests that don't disrupt a person's fundamental rights to privacy.

PARSONS BEHLE & LATIMER

Data Subjects' Rights

- Controllers must:
  - Notify people about how the Controller Processes Personal Data before Processing Personal Data.
  - Give people the ability to access relevant Personal Data Processed by the Controller.
  - Allow people to access their Personal data and correct missing, incomplete, or inaccurate information.
  - Erase information about people upon their request if that information is no longer necessary for the purpose which it was gathered.
  - Restrict Processing.
  - Provide all Personal Data the Controller has about a person to that person in a structured and commonly used, machine-readable format.
  - Allow individuals to object to Processing by automated means, Processing for direct marketing, and Processing carried out in the Controller's legitimate interests.

PARSONS BEHLE & LATIMER

Controller and Processor Obligations

- Controllers:
  - Must implement appropriate technical and organizational measures to protect Personal Data.
  - Incorporate privacy principles such as pseudonymization and data minimization into all Processing activities.
  - Designate, in writing, a representative in the EU if the Controller is not located in the EU but does business in the EU.

PARSONS BEHLE & LATIMER

Controller and Processor Obligations

- Processors:
  - Must contractually guarantee the implementation of appropriate technical and organizational measures to protect Personal Data.
  - Will only Process Personal Data with the Controller's written authorization.
  - Follow specific contractual guidelines such as: ensuring people are authorized to Process Personal Data on the Controller's behalf, implementing appropriate security measures, and assisting the Controller with the Controller's compliance obligations.

PARSONS BEHLE & LATIMER

Controller and Processor Obligations

- Joint Obligations:
  - Create a record of Processing listing the Controller's: contact details, purpose for Processing, categories of Personal Data Processed, categories of recipients, where information transfers, a general description of technological and organizational safeguards.
  - Cooperate with DPAs.
  - Implement appropriate codes of conduct and technical and organizational measures to ensure security measures are tailored to risks presented by Processing.
  - Notify DPAs and affected individuals about data breach events.
  - Carry out Data Protection Impact Assessments ("DPIA") and consult with DPAs where a DPIA reveals a new project, process, or technology could result in high risk to a person in the EU.
  - Potentially appoint a Data Protection Officer within the organization.

PARSONS BEHLE & LATIMER

International Data Transfers

- Generally, Personal Data cannot leave the EU.
- Controllers and Processors can transfer Personal Data out of the EU if the recipient agrees to appropriate safeguards and people in the EU can enforce their rights against the recipients.
  - Appropriate safeguards include: binding corporate rules, standard data protection clauses, and approved codes of conduct.
  - Contractual clauses between the Controller and Processor suffice, but need pre-approval by a DPA.

PARSONS BEHLE & LATIMER

Remedies, Liability, and Penalties

- People in Europe have the right to sue Controllers and Processors.
- Controllers can be sued for damage caused by Processing which infringes the GDPR.
- Processors are liable for damage caused by Processing where it has not complied with the GDPR or acted without their Controller's approval.
- Where more than one Controller or Processor is liable for damages, each Controller or Processor is held liable for the entire damage amount. After payment, the Controllers and Processors sort out who among them are responsible for their share of fault.
- Penalties:
  - For failing to comply with Controller and Processor obligations: €10,000,000 or 2% of annual revenue.
  - For failing to comply with basic principles for Processing, Data Subject Rights, International Data Transfers, Member State laws, and a DPA's orders: €20,000,000 or 4% of annual revenue.

PARSONS BEHLE & LATIMER

What Does This Mean?

- We are on a short time frame for compliance. Starting today, organizations have about 200 days to adopt technical and organizational policies to comply with the GDPR.

PARSONS BEHLE & LATIMER

What Can You Do?

- 0-30 days:
  - Determine whether your organization Processes Personal Data from people in the EU.
  - Determine where that information comes from, what that information is, how you presently secure that information, and whether you share that information with other Controllers, Processors, and other organizations internationally.
  - Review the GDPR, write down its obligations.
  - Determine whether status-quo operations satisfy those obligations and identify gaps.
  - Analyze whether current security processes meet the GDPR's technical and organizational requirements. If not, develop a security plan to achieve compliance.
  - Evaluate current contracts with Controllers and subcontractors. Determine what language should go into contracts with both groups of entities and create a timeframe for revising those contracts.

PARSONS BEHLE & LATIMER

What Can You Do?

- 30 – 90 days:
  - Create a Privacy Office and nominate a data privacy officer.
  - Conduct data mapping exercises to determine how your organization Processes and secures information.
  - Setup a DPIA process that incorporates Privacy by Design principles. Use this process to recommend new technology to comply with GDPR security requirements.
  - Create an Incident Response Plan.
  - Create a data transfer agreement form for internal and external Controllers and Processors.
  - Evaluate Controller and Processor contracts and determine which contracts need revisions to comply with the GDPR.
  - Create Notice and Consent forms compliant with the GDPR.
  - Setup processes to comply with Data Subject Rights.

PARSONS BEHLE & LATIMER

What Can You Do?

- 90 – 180 days:
  - Roll out security plan.
  - Create a Record of Processing; identify the legal basis for processing, and revise contract/processes to find a legal basis for Processing activities. Leverage the data mapping exercise to tie into this exercise.

PARSONS BEHLE & LATIMER

Thank You

- If you have any questions, please contact me at:

Tsutomu Johnson
Tjohnson@parsonsbehle.com
801.536.6903

PARSONS BEHLE & LATIMER