PRIVACY ASSOCIATES INTERNATIONAL LLC

Auditing for the EU's GDPR
A Windfall for Tylenol?

ISACA & IIA Joint Meeting

December 12, 2017

Keith A. Cheresko, Principal **Robert L. Rothman, Principal**

Privacy Associates International LLC

Agenda

- Recap
- GDPR Key Terms
- Controllers and Processors Responsibilities
- Geographic Reach
- Data Subject Rights
- Data Processors
- Data Breach Notification

Recap

Recap

When we last spoke in 2016 we:

- Provided an overview of some of the important changes associated with the EU General Data Protection Regulation – the “GDPR” or the "Regulation”
- Offered suggestions as to what companies should do to get ready

Today

- Reminder that active enforcement of EU GDPR requirements begins May 25, 2018, in 164 days or about 6 months
- EU data protection regulators (Supervisory Authorities) indicate there will be no grace period
- Serious consequences for getting it wrong
- Application of the accountability principle – the obligation to demonstrate compliance through documentation - rests with your organization – are you ready?

PAI

Some GDPR Key Terms

GDPR Key Terms

- **Personal data** - any information relating to an identified or identifiable natural person (data subject); one who can be identified directly or indirectly by reference to an identifier (e.g. name, ID number, location data, online identifiers, IP address or factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that person). (Art. 4(1))
- **Processing** – any operation … performed on personal data. (Art. 4(2))
- **Profiling** – any form of automated processing of personal data to evaluate certain aspects related to a natural person to analyze or predict aspects concerning the natural person. (Art 4(4))
- **Controller** – one that determines the purposes and means of processing personal data. (Art. 4(7))
- **Processor** – one that processes personal data on behalf of another. (Art. 4(8))

PAI

Controllers and Processors Responsibilities

Controllers

- Controllers must implement appropriate technical and organizational measures to ensure and demonstrate processing is performed as required by the GDPR (Art. 24)
- Review measures and update them where and as necessary (Art. 24)
- Include appropriate data protection policies (Art. 24)
- Engage in privacy by design and by default (Art. 25)
- Where necessary appoint a representative in the EU (Art.27)
- Work only with vendors/suppliers (processors) providing sufficient guarantees to implement appropriate technical and organizational measures for processing EU personal data to meet the GDPR
- Enter agreements with suppliers with required terms (Art.28)
- Are there documented procedures and policies in place to demonstrate compliance with these items?

PAI

Processors

- Processors must implement appropriate technical and organizational measures to ensure and demonstrate processing is performed as required by the GDPR (Art. 28)
- Obtain from the Controller prior specific or general approval to hire subcontractors, inform the controller of proposed changes and provide an opportunity to object when changing subs (Art. 28(2))
- Enter into contracts with controllers detailing the processing of EU data subject personal data transactions including the required GDPR contract content (Art.28(3))
- Are there vendor due diligence documented procedures and policies in place and standardized contract clauses in use necessary to demonstrate compliance?

Controller-Processor Contract Requirements

- Contracts between Controllers and Processors relating the processing of EU personal data must legally binding and set forth the:
  - Subject matter and duration of processing
  - Nature and purpose of processing
  - Types of personal data and categories of data subjects
  - Rights and obligations of the controller (Art. 28(3))
- The contract must stipulate that the Processor:
  - Processes personal data only on documented instructions from the Controller, including data transfers

Controller-Processor Contract Requirements

- Informs the Controller of cross border legal requirements before processing
- Requires persons authorized to process the data to undertake confidentiality obligations
- Takes appropriate security measures
- Addresses ability and process for engaging sub-processors
- Assists the Controller in meeting data subjects' data protection rights
- Deletes or returns, at the choice of the Controller, personal data at the end of agreement

Controller-Processor Contract Requirements

- Makes available to the Controller all information necessary to demonstrate compliance with the GDPR including allowing for audits
- Informs the Controller immediately if in the opinion of the Processor the Controller's instructions infringe on GDPR requirements
- Imposes like terms on any sub-processor(s) engaged (Art.28)

- Is there a process to audit new and existing contracts for compliance with these requirements? Is there a procedure or policy addressing formation of new agreements to ensure these contract requirements are addressed?

Accountability

- "The controller shall be responsible for, and *be able to demonstrate compliance* with, [the data processing principles]". (Art. 5(2))
- Personal data processing principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimization
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (Art. 5(1)(a-f))

Lawfulness of Processing

- The right to process personal data is limited. At least one of the following must apply:
  - With data subject's consent
  - For contract performance
  - To comply with legal obligations under EU or member state law
  - To protect the vital interests of a natural person
  - To perform a task in the public interest set out by the EU or member state law
  - For the legitimate interests pursued by the data controller or third party
  - identification and memorialization of the legal basis for processing is necessary to satisfy Article 30 reporting (Art. 6(1)(a-f))
- Does existing procedure address this? Is it documented?

Consent

- Consent, including implied consent, is a basis used by most companies today for processing personal data or transferring it across borders
- Use of Consent is much more limited under the GDPR
  - Must be **freely given** (bargaining power), specific, informed and unambiguous
  - By a statement or clear **affirmative** action
  - Controller has burden of proof

Consent

- Written consent in a document that deals with other matters must be **CLEARLY DISTINGUISHABLE** and must use clear and plain language or it is not valid
- Must be as easy to withdraw as to give
- Contract performance or provision of a service cannot be made conditional on consent, if the processing is not necessary to the performance (Art. 7)
- Do your processes conform? Has adequate notice been given? Are your actual processes and data practices consistent with these requirements and notice given? Is it all documented?

PAI

Geographic Reach

Geographic Reach

- GDPR certainly applies to European processing of EU personal information by European subsidiaries
- More importantly, applies to the processing of European personal data of data subjects who are in the Union by a controller or processor outside the EU (e.g. in the US) where the enterprise is
  - Offering goods or services to data subjects in the EU (regardless of whether payment required) (Art.3(2)(a))
  - Monitoring of behavior or profiling of data subjects in the EU (Art.3(2)(b))

Present Status(?)

- By now (hopefully) a basic review of operations has been conducted:
  - Determined whether subject to the GDPR based on business activities
  - Mapped personal data – what you have, where it came from, and with whom it is shared
  - Understand the legal bases in use for processing, including transferring, EU data subject personal data
  - Understand practices regarding data subject consent
  - Established documented processes and audit procedures to validate practices

Record-Keeping Obligations

- Maintain extensive records of processing activities for controllers (Art. 30)
- Requirements for processors not as extensive
  - Processors are often vendors/suppliers to a controller (you?)
  - Difference based on who directs actions to be carried out on the personal data
- Does audit process assess record keeping practices and verify compliance?

Records of Processing Activities - Controllers

- GDPR imposes record keeping requirements on controllers:
  - Name and contact details of controller, joint controllers, controller's rep. and the data protection officer
  - Purpose for processing
  - Description of categories of data subjects and categories of personal data
  - Categories of recipients to whom personal data have been or will be disclosed including recipients in third countries

Records of Processing Activities - Controllers

- Transfers of personal data to third counties, including identification of the country
- Where possible the envisioned time limits for erasure of the different categories of data
- A general description of the technical and organizational security measures (Art. 30 (1))

- Limited exceptions for entities employing fewer than 250 persons.

Records of Processing Activities - Processors

- GDPR imposes record keeping requirements on processors:
  - Name and contact details of:
    - the processor or processors,
    - each controller on whose behalf the processor is acting,
    - the controller's or processor's rep, and
    - the data protection officer
  - Categories of processing carried out for each controller
  - Transfers of personal data to third counties, including identification of the country
  - A general description of the technical and organizational security measures (Art. 30(2))
  - Limited exceptions for entities employing fewer than 250 persons

PAI

Data Subject Rights

Must Be Able to Accommodate Rights Granted to Individuals

- Detailed Privacy Notices when Data Collected
- Access Rights
- Data portability
- Right to be forgotten

Detailed Privacy Notices when Data Collected

- All the following is required disclosure at the time of Personal Data collection from a data subject:
  - Identity and contact details for the controller
  - Contact details for the data protection officer
  - Purposes for processing as well as legal basis for processing
  - The legitimate interest pursued by the controller or third party (where processing is based the legitimate interest balancing test
  - Recipients or categories of recipients, intent to transfer to third country, existence or absence of adequacy decision by the commission, reference to the appropriate safeguards and the means by which to obtain a copy of them or where they are made available

Detailed Privacy Notices when Data Collected

- Period for which data will be stored or criteria used to determine the period
- Existence of right to request from the controller access to and rectification or erasures of personal data or restrictions of processing concerning the data subject or to object to processing as well as the right of portability
- Where processing based on consent the existence of the right to withdraw consent at any time
- Right to lodge a complaint with a Supervisory Authority

Detailed Privacy Notices when Data Collected

- Whether provision of the personal data is a statutory or contractual requirement to enter into a contract as well as whether data subject is obligated to provide the personal data and of the possible consequences of the failure to provide the data
- Existence of automated decision making, including profiling, and meaningful information about the logic involved as well as significances and the envisioned consequences of the processing for the data subject (Art.13 (1)(2))

- Are privacy notices and actual practices audited to confirm all required disclosures are made and are accurate?

Data Subject Access Rights

Access Rights

- The data subject has the right to obtain from the data controller confirmation whether her personal data are being processed.
- If processing is taking place, the data subject has rights to request the following information:
  - Purposes for processing
  - Categories of personal data processed
  - Recipients or categories of recipients, to whom the personal data has been or will be disclosed, in particular recipients in third countries
  - Period of storage or criteria used to determine period
  - Information regarding the right to request controller rectification or erasures of personal data or restrictions of processing concerning the data subject or to object to processing

PAI

Access Rights

- The right to lodge a complaint with a supervisory authority
- Where data was not collected from the data subject any available information as to their source
- Existence of automated decision making including profiling and meaningful information about the logic involved as well as significances and consequences of the processing for the data subject
- Where data is transferred to a third country the right to be informed of the appropriate safeguards relating to the transfer

- The controller must provide a copy of the personal data undergoing processing (Art.15)
- Are the systems in place adequate to provide the required information upon request?

Data Portability

Data Portability

- The data subject has the right to receive the personal data he provided to the data controller in a structured, commonly used and machine readable format and have the right to transmit that data to another controller without hindrance if:
  - Processing was based on consent or
  - Processing was necessary for a contract and
  - The processing was carried out by automated means
- The data subject has the right to have the personal data transferred directly from one controller to another where technically feasible (Art.20)
- The right is subject to limitations
- Does the organization have in place the ability meet is requirement within the existing IT system?

PAI

Right to Erasure – Right to be Forgotten

Right to Erasure

- The data subject has the right to obtain erasure of her personal data without undue delay and the controller has the obligation to erase personal data where one of the following applies:
  - Personal data are no longer necessary in relation to the purposes for which they were collected or processed
  - The data subject withdraws consent on which the processing is based and there is no other legal basis for the processing
  - The data subject objects to the processing on grounds relating to the data subject's situation where processing was based on certain specific factors, unless the controller demonstrates an overriding interest or it is necessary for the a legal matter involving the controller

Right to Erasure

- The personal data was unlawfully processed.
- Where personal data are processed for direct marketing, the data subject has the right to object at any time to the processing.
- Where the controller made the data public, the controller shall communicate any rectification or erasure of personal data or restrictions on processing to each recipient to whom the personal data have been disclosed, unless impossible or involves disproportionate effort. (Art. 17)

- Are systems in place adequate to prohibit further use of the personal data upon request? Are systems in place for tracking of disclosures to third parties so they can be notified of erasure requests?

PAI

Data Breach

Data Breach Processes Must Comply

- 72 hour period after awareness to notify Supervisory Authority
- No report required when unlikely to result in risk for rights and freedoms of individuals
- Notice to individuals without undue delay where high risk for rights and freedoms (Art. 33)
- Is there an existing incident response program? Have the procedures for addressing incidents involving European personal data been adopted? Tested? Has there been training? Can it be modified to meet the timing requirements?

Privacy Impact Assessments

- Where intended processing is likely to have high impact on privacy
  - Data Protection Impact Assessment (DPIA) required and
  - Where DPIA shows high impact is likely (without mitigating factors) also must have a prior consultation with the DPA (Art. 35)
- Is IT process subject to security policy, practice guidance and audit sufficient to identify need for DPIA? Does policy require? Are DPIA processes incorporated into the IT development process? Is it documented and followed?

Privacy by Design and Default

- Implementation of appropriate measures for ensuring that every data processing complies with principles of privacy by design and default
- Where controller obtains consent for certain data processing activities it must take all measures to ensure that impact on privacy is mitigated
  - Use pseudonimization
  - Limit access and data retention
  - Practice data minimization, etc. (Art. 25)
- Have measures been implemented, documented and followed to meet these requirements?

Privacy of Children

- The default age for giving valid digital consent is set at 16 years in GDPR
- Parental consent required for digital transactions for those under age
- Variation by member state explicitly authorized
- Member states may set own national level as low as 13 (Art. 8)
- Are there appropriate processes in place to address obtaining, honoring and documenting these requirements?

Data Protection Officer

- Mandatory appointment
  - Where processing sensitive data on a large scale
  - Where conducting regular and systematic monitoring of individuals
- Good practice where not mandatory
- Where appointed align function's responsibilities with GDPR requirements (Art. 37)
- Reporting structure and employment protection
- Does audit of practices indicate need for appointment?

Contact Information

Keith A. Cheresko

Privacy Associates International LLC

kcheresko@privassoc.com

www.privassoc.com

(248) 535-2819

Robert L. Rothman

Privacy Associates International LLC

rrothman@privassoc.com

www.privassoc.com

(248) 880-3942