SEYFARTH SHAW

Overview of Current EU Data Protection Directive and Brief Introduction to the EU General Data Protection Regulation (GDPR), Effective May 25, 2018

James Daley, John Tomaszewski, & Jason Priebe

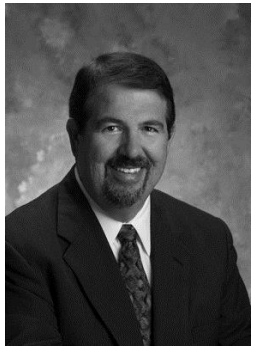
SEYFARTH SHAW

Seyfarth Shaw LLP

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Speakers



James Daley

Senior Counsel
Chicago Office
jdaley@seyfarth.com

John Tomaszewski

Senior Counsel
Houston Office
jptomaszewski@seyfarth.com

Jason Priebe

Partner
Chicago Office
jpriebe@seyfarth.com

SEYFARTH SHAW

What *Is* The GDPR?

GENERAL DATA PROTECTION REGULATION (GDPR)

- Law designed to enhance data protection for EU residents and provide a consolidated framework to guide business usage of personal data across the EU.
  - The GDPR protects the personal data of EU residents, which includes anyone physically residing in the EU, even if they are not EU citizens.
  - The GDPR now extends due diligence obligations and potential liability to Data Processors, not just Data Controllers.
- The deadline for compliance is May 25, 2018.

Analysis of Requirements

- The first step is to gain a high level understanding of your current compliance posture. You need to review a comprehensive list of the requirements, including the following areas:
  - Transparency (i.e., Privacy Policy)
  - Collection and Purpose Limitation
  - Consent
  - Data Quality
  - Privacy Program Management
  - Security in the Context of Privacy
  - Data Breach Readiness and Response
  - Individual Rights & Remedies

New Challenges

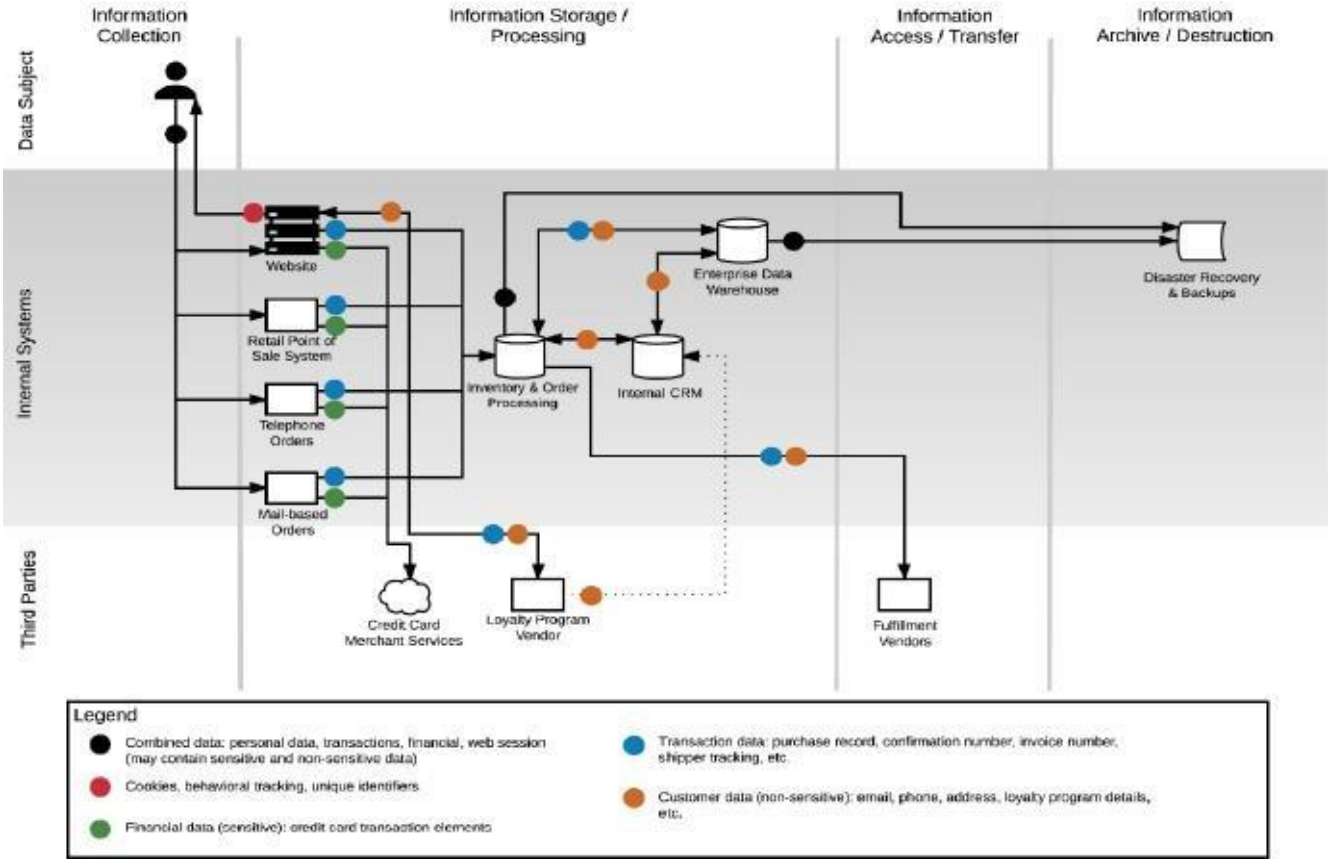
- “Right to be Forgotten”
  - Individuals now have a right to request deletion of their data
  - Businesses will need to make sure they have a way to eoither delete the data, or justify why they refuse such requests
- “Data Portability”
  - Businesses now have to make it “easy” for an individual to move their data from one place to another.
- Significantly Increased Fines (4% of *global* revenue)
- 72 Hour Data Breach Notification Requirement

SEYFARTH SHAW

Initial Steps

Global Data Flow Map

- To ensure you have uncovered all of the risks and appropriately prioritized your plan, you must have a solid understanding of your organization's complete data lifecycle.



Identify Main Establishment

- The ‘one-stop-shop’ concept: where a business is established in more than one Member State, it will have a ‘lead authority’, determined by the place of its ‘main establishment’ in the EU.
- Where an organization has multiple establishments, the lead authority is determined by where the decisions regarding the purposes and manner of the processing in question takes place
- If decisions are actually taken in another establishment in the EU, the authority of that location is the lead authority.
  - Execute intra-group governance documents supporting obligations.

Allocate Budget & Resources

- Senior management should be made aware of the changes to data protection law and how it will affect your business.
- Senior management should designate the individuals that will formulate a plan for how your business will implement the requirements of the GDPR and will educate the wider workforce on its operational impact.

Date Protection Officer

- Under Article 37 of the GDPR, a Data Protection Officer (DPO) must be appointed where the core activities of the controller or the processor involve “regular and systematic monitoring of data subjects on a large scale” or where the entity conducts large-scale processing of “special categories of personal data.”

  – The DPO may be an employee or a third party service provider
  – Should be a direct report “to the highest management level”
  – Shall operate with significant independence

SEYFARTH SHAW

Action Items

Privacy Impact Assessments

- Given the vast amounts of data being collected and processed by organizations these days, creating a comprehensive Data Map can be challenging – BUT, it is a requirement under the Regulation

- A structured and planned approach including the following steps:
  - Appointing a person/ team responsible for creating and maintaining the PIA.
  - Defining a Project Plan.
  - Gathering relevant information.
  - Preparing the PIA based on the gathered information.
  - Prioritize systems and functions involving Personal/Sensitive Data
  - Maintaining and updating the PIA

Identify Legal Basis for Processing

- Under EU data protection law, there must be a lawful basis for all processing of personal data (unless an exemption or derogation applies).
- A controller may process personal data where the controller has a legal obligation to perform such processing.
  - The legal obligation must apply to the controller, and must be binding in nature.
  - As the WP29 has pointed out on several occasions, a "legal obligation" in this context means a legal obligation arising under EU law or the laws of a Member State. A legal obligation to process personal data arising under the laws of a non-EU jurisdiction.

Develop Policy Controls Around Authorities

- The GDPR requires national data protection authorities (Supervisory Authorities) to respond to complaints and enforce the GDPR and local data protection laws where only data subjects in that member state are affected.

- GDPR creates the requirement to maintain detailed records of an organization's data processing activities and to make these records available to supervisory authorities on request.

Formalize Data Processing Register

- The written record of processing activities - data processing register.

- Map and risk rank the current data processing activities.
  - Review whether data subject consent forms, privacy notices and policies and data transfer mechanisms are adequate to meet data processing requirements and develop a plan to replace them.
  - Seek to limit liability by baking into contracts minimum required data processing obligations, including provisions restricting appointment of sub-processors without the consent of controllers.

Develop Privacy Notices

- Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

- The starting point of a privacy notice should be to tell people:
  - who you are;
  - what you are going to do with their information; and
  - who it will be shared with.

Identify & Implement Joint Controller Policies

- In circumstances where two or more parties determine the purposes for which and the manner in which the personal data is processed, each party will be a controller and will be liable for the entirety of any damage to a data subject, unless they can prove they were not in any way responsible for the event giving rise to the damage.

  – Consider whether there are any intra-group, customer or service provider arrangements where a group company is a joint controller.
  – Ensure that contract negotiators are aware of the default position of each controller being liable for the entire damage to a data subject if it is in any way responsible for the event giving rise to the damage and include appropriate cross indemnification

Develop Standard Process, Application

- Start with the results of the Gap Assessment and Risk Analysis, build a project plan for each functional area within the business with a timeline of completion.

- Privacy Impact Assessment (PIA) will be present as a standard process in maintaining and ensuring the relevant privacy and data protection levels.
  - Regulation requires organizations to perform this process in projects dealing with personal data in order to evaluate the risks.

Develop Process to Demonstrate Consent

- The GDPR is clear that you must be able to demonstrate that consent was given.
  - Consent must be “freely given, specific, informed and unambiguous.”
  - Consent cannot be inferred from silence, pre-ticked boxes, or inactivity.
- Data subjects have the right to withdraw consent at any time.
- The GDPR adds a presumption that consent is *not* freely given if there is “a clear imbalance between the data subject and the controller.”
- Consent must be specific to each data processing operation.

Develop International Implementation Process

- The concept of the data processor is well known from the Data Protection Directive. Although processors have several obligations, one of the most notable is:
  - Implementation of sufficient security measures, having regard to the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.

- In practice, organizations will be expected to put into place comprehensive but proportionate governance measures, including implementation of data protection by design and by default.

Develop Process to Cooperate With DPA

- National Data Protection Authorities ("DPAs") are appointed to implement and enforce data protection law, and to offer guidance.
- DPAs are responsible for enforcing data protection laws at a national level, and providing guidance on the interpretation of those laws.
- Companies will need to cooperate with DPA investigations, including on-site visits. An organization must cooperate with DPA when it has voluntarily submitted to the oversight by DPA or when the processing concerns employee data.

Develop Analysis Tools

- Truly complete identification and deletion of personal information is challenging. That's because the mainframe environments at these large enterprises typically store data in many different places—and the dependencies between these different data repositories are often complex and poorly documented.
- A number of data management and analysis tools to make data easier to use.
- Such tools include:
  - data visualization
  - expansion of dashboard interfaces
  - proliferation of augmented reality devices

Develop Process to Communicate Results

- In order to ensure that personal data are processed fairly, EU data protection law obliges controllers to communicate transparently with data subjects regarding the collection and further processing of their personal data.
  - Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data.

Train Senior Management/ P/C Managers

- Senior management should be made aware of the changes to data protection law and how it will affect your business.
- Senior management should designate the individuals that will formulate a plan for how your business will implement the requirements of the GDPR and will educate the wider workforce on its operational impact.
- The Working Party's guidance also states that if an organization's management do not agree with and decide not to follow a DPO's recommendation then they should formally record this and the reasons for their decision.

Train Senior Management

- Senior management should be made aware of the changes to data protection law and how it will affect your business.
- Senior management should designate the individuals that will formulate a plan for how your business will implement the requirements of the GDPR and will educate the wider workforce on its operational impact.

Standardize Process to Manage Vendor(s)

- Any processing of personal data by a third-party vendor should be in scope for a GDPR-compliant vendor-management process, regardless of the cost of the service offering.

- The broad strokes of applying a constructive approach to vendor management include:
  - identifying the right people
  - formulating a process for interfacing with vendors
  - leveraging technology to manage the process keeping solid metrics for internal and external compliance purposes.

Develop Individualized Processes

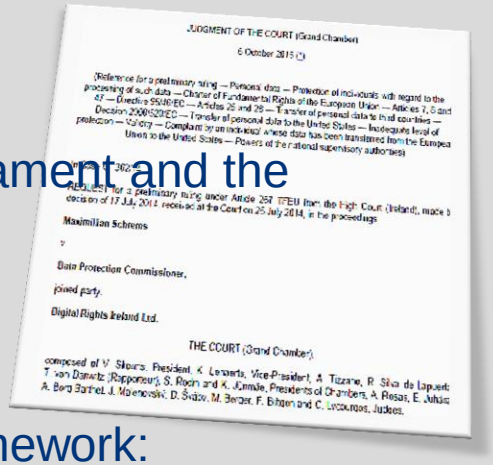
- Higher client expectations, individualized processes as well as the ability to handle increasing complexity through the application of new technologies are causing a paradigm shift in supposedly standardized auditing.
- Advisory plays an essential role throughout the process.
- Individualized approaches call for auditors and advisors with a more broadly-based specialization.

Security Breach Response Process

- In the event of a breach, a company should take the following general steps:
  - Consult your company's Security Breach Management Plan.
  - Contact the pre-assigned Response Team.
  - Identify what breach has occurred and take appropriate steps.
  - Consider your notification requirements.
  - Consider the Public Relations implications and your response (if any).
  - Record all actions taken.
  - Review the outcome of the breach and the effectiveness of your response.
  - Plan on how such a beach can be avoided in the future.

Additional Resouces

- Safe Harbor Decision: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN
- Art. 29 WP Statement: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
- Position Paper of the German DPAs: https://datenschutz-berlin.de/attachments/1150/Positionspapier_DSK.pdf
- Communication from the Commission to the European Parliament and the Council, 6 November 2015: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf
- EC press release regarding new EU-US Privacy Shield Framework: http://europa.eu/rapid/press-release_IP-16-216_en.htm


JUDGMENT OF THE COURT (Grand Chamber)

6 October 2015 (*)

(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)

In Case C-362/14,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

Maximillian Schrems

v

Data Protection Commissioner,

joined party:

Digital Rights Ireland Ltd,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), S. Rodin and K. Jürimäe, Presidents of Chambers, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen and C. Lycourgos, Judges,

SEYFARTH SHAW

Thank You