RELATIVITY FEST

OCT 22 - 25, 2017
CHICAGO, US

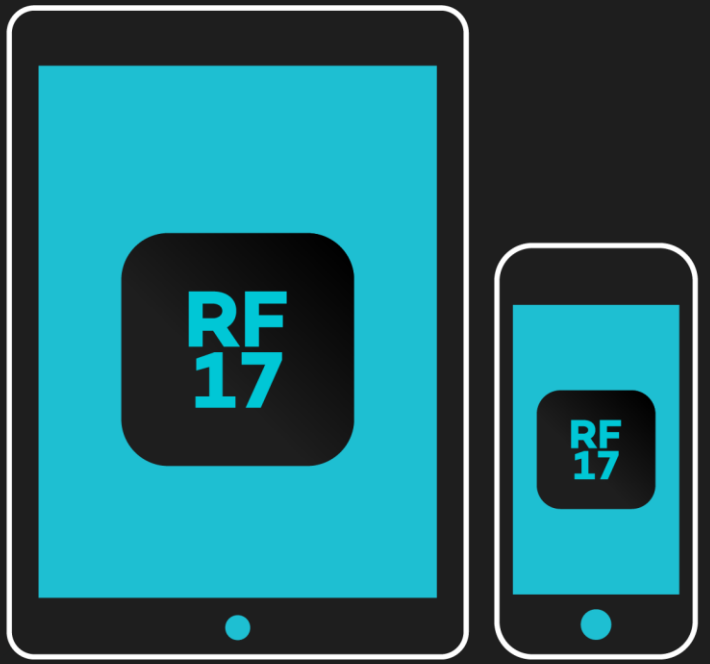
A Practical Roadmap for EU Data Protection and Cross-Border Discovery - LIE115992

Download the RF17 Mobile App

Find your favorite speakers, set your agenda, connect with new friends, and more. Get it in the App Store or Google Play.

Download on the App Store

GET IT ON Google Play



Jason Priebe

Partner Seyfarth Shaw LLP
jpriebe@Seyfarth.com

Natalya Northrip

Counsel Seyfarth Shaw LLP
nnorthrip@Seyfarth.com

Agenda

- Transitioning from EU Data Protection Directive to the EU General Data Protection Regulation (GDPR)
- Challenges Presented by the New Rights for Individuals Under the GDPR
- Privacy by Design and by Default
- Data Security Breach Requirement
- Data Protection Officer (DPO) Requirement
- How Will the GDPR Affect Cross-Border Discovery?

Transitioning from EU Data Protection Directive to the EU GDPR

EU General Data Protection Regulation (GDPR)

- The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC.
- 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.
- Compliance date is **May 25, 2018.**
  - After this date, non-compliant organizations may face enforcement and significant fines that will depend on the nature and severity of the violation, up to 20,000,000 Euros or 4% of **Global** turnover (net) income.

Transitioning from EU Data Privacy Directive to the GDPR

	Directive 95/46/EC	GDPR
Authority	Required Member States to implement its principles through national legislation	GDPR is the law in all Member States; no national implementation is required
Application	Applies to data controllers only	Applies to data controllers, processors, and sub-processors
Enforcement	Inconsistent enforcement from state to state; low penalties	Bet-the-company sanctions
Data Protection Officers	Not required	Required for companies meeting certain criteria (under which most large companies will qualify)
Consent	Varying types of consent	Explicit consent only
Definition of Personal Data	Limited	Expanded to include location data, online identifiers, and genetic data
Data Privacy Impact Assessment	Suggested	Required when collecting and processing sensitive or great in volume personal data
Privacy Notice	Required with suggested language	Required with specific language
Breach Notification	Not required	Required within 72 hours

Analysis of Requirements

- Understand your organization's current compliance posture by analyzing the GDPR list of 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

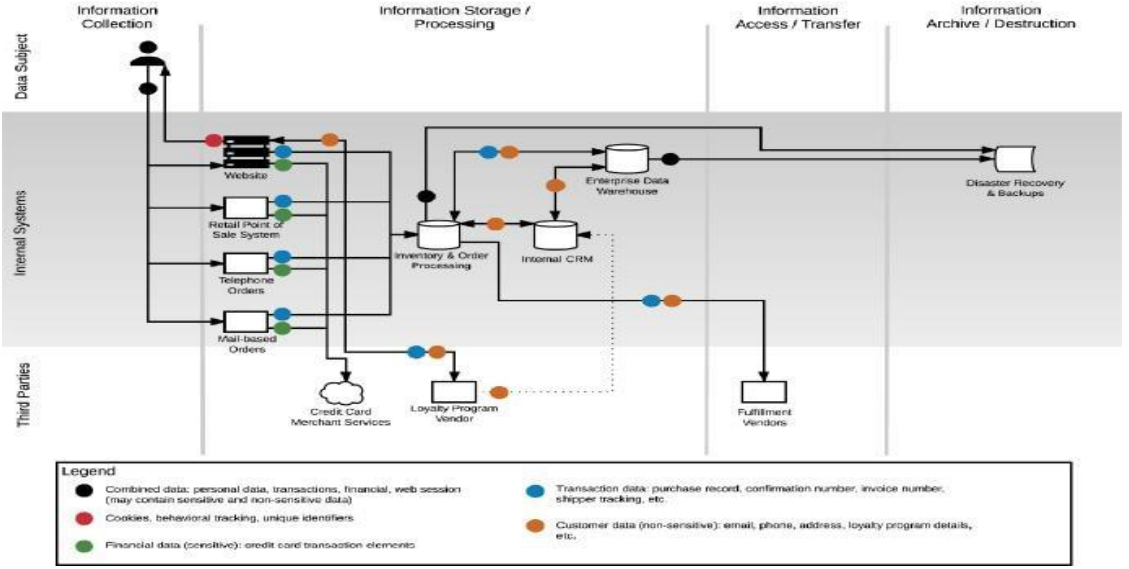
Privacy Impact Assessment (PIA)

- 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.

Global Data Flow Map

- Uncover the risks and appropriately prioritize your preparedness plan by obtaining 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.
- The GDPR will be enforced more strictly than the current Data Protection Directive.
- The EU Data Protection Authorities (DPAs) are increasing their budgets and workforce to police GDPR compliance.
  - E.g., the Irish Data Protection Commissioner (DPC) announced a 59% budget increase and plans to double its staff.
- Prepare to demonstrate compliance (record keeping).

Challenges Presented by the New Rights for Individuals Under the GDPR

New Rights for Individuals Under the GDPR

- **The right to be informed.**
- The right of access.
- The right to rectification.
- **The right to erasure.**
- The right to restrict processing.
- **The right to data portability.**
- The right to object.
- Rights in relation to automated decision making and profiling.

The Right to Be Informed

Complying with The Right to Be Informed

- The GDPR requires organizations to supply certain information to individuals, including:
  - Identity and contact details of the controller and the Data Protection Officer (DPO).
  - Purpose of the processing and the lawful basis for the processing.
  - Cross-border transfer details and safeguards.
  - The existence of each of data subject's rights.
  - The right to withdraw consent at any time.
  - The right to lodge a complaint with a Data Protection Authority (DPA)
  - Categories and sources of personal data (but only if not obtained directly from data subject).
  - The existence of automated decision making, including profiling, the significance and the consequences.

Complying with The Right to Be Informed

- When should information be provided?
  - When data is obtained directly from data subject – at the time of collection.
  - When data is not obtained directly from data subject:
    - Within a reasonable period of having obtained the data (one month).
    - If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
    - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- The information provided to the data subject about must be:
  - Concise, transparent, intelligible and easily accessible;
  - Written in clear and plain language, particularly if addressed to a child; and
  - Free of charge.

The Right of Data Erasure (i.e., the Right to Be Forgotten)

Complying with The Right to Erasure

- Not an absolute right. Applies only in specific circumstances, including:
  - Where the personal data is no longer necessary for the purpose for which it was originally collected/processed.
  - When the individual withdraws consent or objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - The personal data was unlawfully processed (i.e., otherwise in breach of the GDPR).
  - The personal data has to be erased in order to comply with a legal obligation.
- May refuse to comply with erasure request where the personal data is processed:
  - To exercise the right of freedom of expression and information.
  - To comply with a legal obligation, or for exercise of official authority.
  - For public interest reasons (public health, archiving or statistical purposes, scientific research).
  - Exercise or defense of legal claims.

Complying with The Right to Erasure

- Prepare process and procedures for responding to erasure requests.
- When receiving an erasure request, evaluate whether compliance is required (i.e., are you permitted to continue processing because of an exception).
- Revisit your contracts with third-parties to obligate them to assist you in handling erasure requests with respect to personal data you transferred to them.
- Document each erasure request, investigation, and resolution.

The Right to Data Portability

Complying with the Right to Data Portability

- The right to data portability only applies:
  - to personal data an individual has provided to a controller;
  - where the processing is based on the individual's consent or for the performance of a contract;
  - when processing is carried out by automated means.
- Data portability covers the subject's personal data that he or she *provided* to a data controller.
  - Includes data actively and knowingly provided by the data subject (e.g., mailing address, user name, age) and observed data that is "provided" by the data subject by virtue of the use of the service or the device (e.g., search history, location data).
  - Does not include "inferred" data, i.e., data generated by the subsequent analysis of the data subject's behavior.

Complying with the Right to Data Portability

- Controllers should offer a direct download opportunity in a structured, commonly used and machine readable form
- Controllers should allow for direct transmission to another controller if technically feasible.
- **Retention:** No obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period.
- **Timing:** Data controllers must answer a portability request "without undue delay" and in any case "within one month of receipt of the request"
  - 3 months for complex cases, but inform data subject of the delay within 1 month of the original request.
- **Security:** When transferring data, the data controller is responsible for taking "**all the security measures"** needed for secure transmission (e.g., by use of encryption) to the right destination (e.g., by use of additional authentication information).

Privacy by Design and by Default

Privacy by Design and by Default

- Article 25 requires controllers to implement “data protection by design and by default” requirements, including:
  - integrate appropriate technical and organizational safeguards:
    - at the time of the determination of the means for processing; and
    - at the time of the processing itself.
  - process only personal data which are necessary for each specific purpose of the processing, considering:
    - the amount of personal data collected;
    - the extent of their processing, the period of their storage and their accessibility.

Privacy by Design and by Default

- Ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle:
  - building new IT systems for storing or accessing personal data;
  - developing legislation, policy or strategies that have privacy implications;
  - embarking on a data sharing initiative; or
  - using data for new purposes.

Privacy by Design and by Default

- Develop and implement a Privacy Impact Assessment tool for the Business to complete each time it designs or procures a new data-processing system.
- Analyze data collection forms (e.g., web pages) to ensure that only data necessary for the purpose is collected.
- Automate data deletion processes, in accordance with your organization's records retention schedule, to ensure that personal data is automatically deleted at the end of its lifecycle.
- Analyze third-party data processor contracts to address how responsibility and liability for the implementation of "privacy by design" and "privacy by default" requirements will be addressed.

Data Security Breach Requirement

Data Breach Response

- Under the GDPR, breach notifications are **mandatory:**
  - to the local Data Protection Authority (DPA) within 72 hours; and
  - to the affected data subjects “without undue delay.”
- **UNLESS** the breach “is unlikely to result in a risk for the rights and freedoms of individuals” (e.g., anonymized or encrypted data).
- Any data-breach investigation and resulting determination regarding reporting must be documented.
- Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Data Breach Response

- Minimize personal data at collection stage.
- Do not keep personal data longer than required under the retention policy or legal hold.
- Update the retention policy and records retention schedule.
- Critically evaluate each retention period for each record category.
- Have a designated and trained Security Incident Response Team (SIRT) in place.
- Establish individual notification procedures.

Data Breach Response

- In the event of a breach, an organization should take the following general steps:
  - Consult your organization'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.

Data Protection Officer (DPO) Requirement

Data Protection Officer (DPO) Requirement

- The GDPR requires some, but not all, companies to appoint DPO.
- Under Article 37 of the GDPR, a DPO is required for a private sector organization in two specific cases:
  - Where the **"core activities"** of the controller or the processor consist of processing operations, which require **"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."**
- Determine whether your organization is required to appoint a DPO.
- If yes, identify, vet, and appoint a DPO by the May 25, 2018 deadline.

Data Protection Officer (DPO) - Qualifications

- 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
  - Necessary levels of organizational seniority, autonomy, and influence in order to play a key role in implementing the essential elements of the GDPR.
- Shall have expert knowledge of data protection law and practices.
  - Expertise level commensurate with the sensitivity, complexity and amount of data.
- Shall have in-depth understanding of the GDPR.

How Will the GDPR Affect Cross-Border Discovery?

How will GDPR Affect Cross-Border Discovery?

- Life As we Know It: The EU Directive (in effect since 1995) has Existing Restrictions
  - Processing
  - Transfers
- GDPR Ups the Ante and Changes the Game
  - Increased accountability
  - Processors have increased roles and liability
  - Consent has been clarified and bolstered
  - Pseudonymisation has increased in favor and preference
  - Enhanced Data Subject rights
  - Policies and Procedures needed to Demonstrate Compliance
  - More vectors of enforcement (SAs, data subjects, interest groups and NGOs, for starters)

Documentation is the Key to Accountability

Follow Your Pre-Established Standards and Documentation Before the Fact

Example to Consider for Processing Activity:

- Document the legitimate and lawful interest you are pursuing
- Describe the processing and its legitimate purposes
- Document and assess the data subject rights affected and measures taken to avoid risk
- Assess the necessity and proportionality of processing (data minimization, psudonymisation)
- Describe safeguards and security measures to protect data
- Establish the timeframes of use, retention and erasure
- Identify all recipients of personal data
- Document the data subject notification, consultation and consent process, if applicable, including documentation to demonstrate any consent was informed and voluntary.

(all before you even think about a transfer to a country without “adequate protections”!)

Let Us Know What You Think

You'll receive a short survey via email for each breakout session and the overall event. Please take a minute to tell us what you think.

Meet Our Sponsors

Visit our sponsors in the Community Pavilion to learn about their services and Relativity integrations. Submit your completed sponsor passport for the chance to win one of three Relativity Fest passes.