GDPR at Nine Months: Experiences and What's Next

K Royal | Director, Consulting | TrustArc

Mia Singer | Principal and Owner | Singer Consulting, LLC

Session Structure

- General scope and breadth of the GDPR
- Major challenges and potential solutions to compliance with the law
- GDPR became effective May 25, 2018—what does ongoing compliance and enforcement look like?

General Data Protection Regulation

- Why did the European Commission adopt the GDPR?
  - The Data Protection Act/Directive was implemented in 1997
  - Regulation vs. Directive
  - Two year transition from passage of the law to implementation on May 25, 2018
  - Consistent framework for data protection across the EU
- Data protection structure for all European residents
  - Affects companies without offices/employees in EU countries
  - Not a data transfer mechanism but affects data transfer
- Why is this topic on the minds of board members and executives?
  - Customer and vendor requirements
  - 4% of annual turnover

GDPR Definitions – Personal Data and Sensitive Personal Data

- Personal Data—Any information that relates to a living identified or identifiable individual
  - Individual can be identified or are identifiable directly from the information in question or can be indirectly identified from the data in combination with other information
  - Extremely broad—Name, address, IP address, user id, employee number
  - Racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic and health data
  - Requires lawful reason in addition to a separate condition to process
- Sensitive Personal Data—A data element that relates to a living identified or identifiable individual that creates a higher risk if disclosed

GDPR Definitions—Controller vs. Processor

- The Data Protection Directive primarily addressed controllers and did not restrict processors as directly
- A data controller determines the purposes and means of processing personal data
- A data processor is responsible for processing/accessing/using personal data on behalf of a controller

GDPR Principles - Lawfulness, Fairness, and Transparency

- Documentation and consents must clarify the purposes for collecting data
- Must identify the lawful basis for processing (must have one)
  - Consent—Must be voluntarily given, specific
  - Performance of a Contract- Take steps at the request of the subject
  - Legal obligation – Compliance with a legal obligation to which the controller is subject.
  - Vital interests—protect someone's life (health context)
  - Public task—generally public authorities
  - **Legitimate interests**—most flexible basis
- Special category data—lawful basis and separate condition
- Criminal offense data
- Fair processing—not unduly detrimental, unexpected or misleading
- Transparent—open and honest with people about data use

GDPR Principles of Data Collection and Storage

- Data Minimization
  - Adequate to fulfill your stated purpose
  - Relevant—link to purpose
  - Limited to what is necessary
- Storage Limitation
  - Limit retention of data to meet purposes
  - Review data held and evaluate for destruction
- Right to be forgotten/data deletion
  - Subject Access rights include the right to erasure

Other Rights of Data Subjects

Right of access by the data subject (Art 15)	Rectification (Art 16)	Restrictions of processing (Art 18)	Portability (Art 20)	Objection (Art 21)	Automated decision-making (Art 22)
Confirmation that their data is being processed; access to their personal data; and other supplementary information	Rectify/Edit any errors in their personal data or have incomplete data completed	Restrict the processing when accuracy of the data is contested, the data is no longer needed for the purpose or the processing is unlawful	Request copies of personal data in a structured, commonly used and machine-readable format. Ability to request transfer to another business (e.g., to move data from one online platform to another)	Right to object to processing when it is based for direct marketing purposes or on legitimate interest grounds.	Right not to be subject to a decision based solely on automated processing.

GDPR Principles - Security

- Integrity and Confidentiality
  - Must have appropriate security in place
  - Confidentiality, integrity, and availability
  - Physical security and cybersecurity
    - Use encryption and pseudonymization when possible
  - Maintain policies and processes to test effectiveness
- GDPR Articles 33 and 34 create a new obligation for companies to notify the relevant supervisory authority and potentially affected data subjects when a security breach occurs that impacts EU residents:
  - Article 33 requires notification to supervisory authorities within 72 hours of a breach being identified.
  - Article 34 requires that notification occurs 'without undue delay' to data subjects where there is a high risk to their rights and freedoms being impacted.

Accountability and Implementation

- Must create technical and organizational measures to meet the requirements of accountability
  - Privacy by design and default approach to data governance
  - Data protection policies
  - Written contracts in place with organizations that process personal data
  - Document processing activities
  - Implement appropriate security measures
  - Recording, and, where necessary, reporting PD breaches
  - Privacy Impact Assessments must be done for uses of PD that are higher-risk
  - Appoint a Data Protection Officer
- Penalties for noncompliance are up to 4% of organization's annual turnover

Strategy for Compliance

- How is the GDPR enforced?
  - Data Protection Authorities in each country directly interact with controllers and processors to determine violations and enforce the GDPR
- Determine responsibility and staffing for the program
  - Do you need a Data Privacy Officer (DPO)?
    - Public authority or entity
    - Processing activities consistently involve large-scale monitoring of individuals (behavior tracking)
    - Processing activities involve sensitive data or data related to criminal convictions or offenses
    - If no DPO is needed, ensure that privacy program is sufficiently staffed and that there is a primary contact for Data Processing Authorities to contact
  - If no DPO is needed, ensure that the privacy program is sufficiently staffed and that there is a primary contact for national DPAs to contact.

Strategy for Compliance, continued

- Determine details regarding personal data
  - What elements are collected, retained, transferred, processed?
  - Where and how are they stored?
    - Owned data center, cloud provider, encryption, etc.
  - What systems are involved in the collection, retention, transferring, and processing of the data? What internal departments own the data?
  - Create a data map of what is held, and how it is protected and used
  - If personal data is transferred to other entities for processing, determine details regarding the data, and the processing

Strategy for Compliance, continued

- Policies, Contracts, and Analyses (Document, Document, Document)
  - Create Privacy Policies and review other applicable policies and contracts to ensure that appropriate terms regarding data collection, protection, and processing are in place
    - Customers
    - Employees
    - Vendors
    - Websites
  - Review contracts with vendors/Data Processors and replace or amend as needed to ensure that the data to be transferred is described, uses of the data are proscribed, and that the level of protection of data is clear.
  - Document lawful bases to process data
  - Conduct any Privacy Impact Assessments regarding close calls for data use

Strategy for Compliance, continued

- Ensure that your organization has adequate security in place for each system based on the type of data held in the system and the types of uses of the data
- Comply with general data breach notification obligations
  - Prepare data breach response plans before needed
- Evaluate data transfer mechanisms
  - If organization transfers EU personal data outside of the European Economic Area to a country that is not recognized as providing an adequate level of data protection, another structure to ensure protection of data is required:
    - Privacy Shield Certification (replaces Safe Harbor)
    - Binding Corporate Rules

Strategy for Compliance, continued

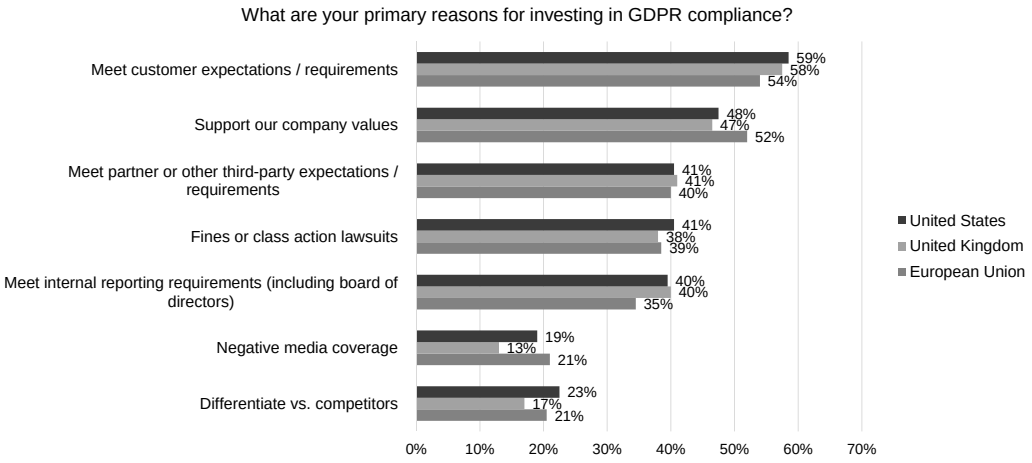
- Audit all facets of data privacy program
  - Compliance with GDPR is an ongoing effort
  - Update policies, procedures, and analyses as needed
  - Ensure that contract templates create privacy by default on a going forward basis

What enforcement has occurred thus far?

- Many organizations do not report being ready for GDPR enforcement
  - Those who have completed the compliance process are largely pleased with what they have learned and implemented
- DPAs have increasingly become more active
- Complaints have increased
  - Generally filed against data-rich companies (Google, Facebook)
  - The number of complaints to the UK's data protection watchdog has more than doubled since the end of May
  - Many companies have received data subject requests

What Motivates Companies to Comply

Motivated more by values and customer expectations than fear of fines



17

Motivation to Comply

- Before May 25, 2018
  - Driving factor was harsh penalty amounts
  - How to get your executive
  - How to engage Board

- Now
  - Customer requests
  - Partner assurances
  - Corporate values

18

What is next?

- Brexit
  - Draft UK Withdrawal Agreement provides for EU data protection law to be in place until December 31, 2020.
- ePrivacy Directive
- California Consumer Privacy Act of 2018
- Evaluation of GDPR compliance for multi-national companies
  - Other countries and US states increasing protections
  - A consistent world-wide approach may make sense
- Enforcement actions are accelerating