EU General Data Protection Regulation for Compliance Professionals

Frank Morgan
Deputy Chief Privacy Officer, Lockheed Martin

EU GENERAL DATA PROTECTION REGULATION

- What is the GDPR?
- Your Role in GDPR Compliance
- Key GDPR Articles
- Complying with Data Subjects Rights Requests

GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) intended to strengthen and unify data protection for all individuals within the European Union. It also addresses the export of personal data outside the EU.

The GDPR is the first major EU-wide data privacy law update since 1995 and replaces the current EU General Data Protection Directive.

The GDPR is considered an accountability and risk-based regulation. This means organizations must implement appropriate policies and procedures and other accountability mechanisms taking a risk-based approach.

The GDPR includes 99 Articles, 39 of the Articles require evidence of a technical or organizational measure to demonstrate compliance. The accountability principle in Article 5(2) of the GDPR requires organizations to demonstrate compliance with the principles of the GDPR.

MEMBER STATE LAWS

Countries that have passed a GDPR Implementing Law		
Austria	Belgium	Croatia
Cyprus	Denmark	Finland
France	Germany	Hungary
Iceland	Ireland	Italy
Latvia	Liechtenstein	Lithuania
Luxembourg	Malta	Netherlands
Norway	Poland	Romania
Slovakia	Spain	Sweden
United Kingdom		
Countries that have GDPR Implementing Bills under consideration by their national legislatures		
Bulgaria	Czech Republic	Estonia
Greece	Portugal	Slovenia

Map Source: NYMITY

MEMBER STATE LAWS

- **Draft Bills:**
  - **Bulgaria** - Draft Law on Amendment and Supplement to the Personal Data Protection Act
  - **Czech Republic** - Data Protection Bill and Bill Amending Other Laws and Amendments to Draft Government Bill 138/12 on the Protection of Personal Data
  - **Estonia** - Personal Data Protection Act 2018
  - **Finland** - Amendments to the Draft Proposal for Supplementing the GDPR
  - **Germany** - Draft Second Law on the Adaptation of Data Protection Law to the GDPR
  - **Greece** - Law on the Protection of Personal Data Pursuant to Regulation (EU) 2016/679
  - **Portugal** - Proposed Law 120 XIII - Data Protection Law Proposal
  - **Slovenia** - Proposal of the Law on Personal Data Protection
  - **Spain** - Draft Organic Law for the Protection of Personal Data and Guarantee of Digital Rights

"May 25th marks the end of the beginning, a lot of work remains to be done."

~ Elizabeth Denham, UK Information Commissioner (April 18, 2018)

During a panel session on GDPR enforcement, CNIL Director of Rights Protection and Sanctions Directorate Mathias Moulin did not mince words, warning that the time for the GDPR's transition "is coming to an end," and that it's "time for action" and there will be "teeth."

YOUR ROLE IN GDPR COMPLIANCE

- Develop GDPR fluency
- Document roles & responsibilities
- Build an internal cross-functional Privacy network
- Assess your environment
- Training & Awareness

KEY GDPR ARTICLES FOR COMPLIANCE PROFESSIONALS

- Article 13 — Notice to Data Subjects
- Article 15 — Right of Access by the Data Subject
- Article 33 — Notice of Personal Data Breach
- Article 35 — Data Protection Impact Assessment

- Article 88 — Processing in the context of employment

GDPR ARTICLE 13 – NOTICE TO DATA SUBJECTS

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- the identity and the contact details of the controller;
- contact details of the Data Protection Officer;
- the purposes of the process… ;
- where the processing is based… ;

Takeaway Action: Review External and Internal Privacy Notice(s)

GDPR ARTICLE 15 – RIGHT TO ACCESS BY THE DATA SUBJECT

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information…

- Purpose of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- Period for which the personal data will be stored;
- Right to request from the controller rectification or erasure of personal data;
- Where the personal data are transferred to a third country… the data subject shall have the right to be informed;

The controller shall provide a copy of the personal data undergoing processing.

Takeaway Actions: Create cross-functional process and test!

GDPR ARTICLE 33 – NOTICE OF PERSONAL DATA BREACH

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…

Takeaway Actions: Ensure your function is included in Incident Response Plan.
Test your process (can you comply with 72-hour notification requirement?).

GDPR ARTICLE 35 – DATA PROTECTION IMPACT ASSESSMENT

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Takeaway Actions: Ensure 'your' processes have a DPIA.
Document DPIA process.
Review current DPIA questionnaires for completeness.

GDPR — DEROGATIONS

Article 88 — Processing in the context of employment

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment…

Takeaway Action: Monitor member state legislation.

RESOURCES

International Association of Privacy Professionals (IAPP)

- iapp.org

NYMITY — provides privacy compliance, research, and risk management solutions for organizations

- nymity.com

GDPR

- http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf