INFORMATION PRIVACY LAW COURSE SERIES

GDPR and European Privacy Law Part II:
GDPR Rights, Obligations, and Data Transfer

OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS UNDER THE GDPR

Data Protection Officer (DPO)

GDPR Articles 37, 38, 39

All controllers and processors whose core activity involves regular monitoring of people or processing large quantities of personal data must designate a data protection officer (DPO). Public agencies and authorities that engage in these same core activities must designate a DPO.

DPOs are to inform their organizations about their obligations under the GDPR, to monitor compliance with the regulation, to provide for privacy awareness training for the workforce, and to cooperate with Supervisory Authorities. DPOs must also field questions and concerns raised by data subjects.

DPOs must be independent, must report to the "highest management level," and cannot be penalized for carrying out their duties.

Security

GDPR Article 32

Controllers and processors implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Data Protection by Design and Default

GDPR Article 25

Data protection must be built in starting at the beginning of the design process. Data protection cannot be an afterthought and must be documented.

The data controller must implement measures to ensure that by default, only personal data necessary for each specific purpose of the processing are processed. Default settings should be set so that personal data aren't accessible to an indefinite number of people.

Records of Data Processing Activities

GDPR Article 30

Data controllers and processors must create and maintain a documented register of all activities they do that involve processing of EU personal data. Documentation must be kept about categories of data subjects, personal data, recipients of personal data, the purposes of the processing, transfers to third countries, security measures implemented, among other things.

Organizations with fewer than 250 employees are exempt from this requirement unless the processing is likely to result in a risk to the rights and freedoms of data subjects or includes sensitive data or data relating to criminal convictions or offenses.

Data Protection Impact Assessments (DPIA)

GDPR Article 35

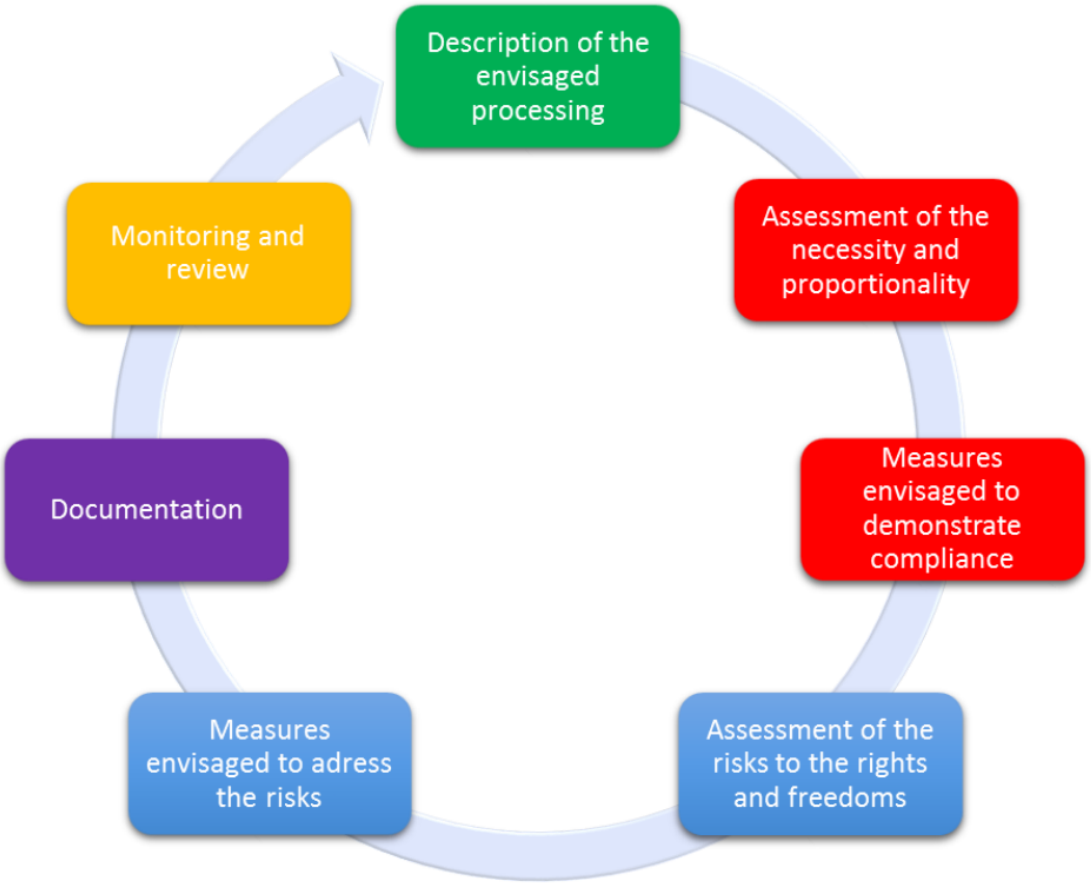
In situations designated as "high risk," data controllers and processors must conduct a data protection impact assessment (DPIA). A DPIA must contain information about the nature and purpose of the processing, an assessment of the necessity and proportionality of the processing in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, and the measures and safeguards to address the risks. According to the Article 29 Working Party, "Carrying out a DPIA is a continual process, not a one-time exercise."

The Article 29 Working Party has identified factors that increase the degree of risk. These factors include:

- evaluation or scoring, especially when profiling and predicting
- systematic monitoring
- processing of sensitive data
- large scale processing
- combining separate datasets
- processing affecting vulnerable individuals
- innovative uses or technologies
- transfers of data to countries outside the EU
- inhibiting data subject rights

The GDPR states that controllers should seek the views of data subjects where "appropriate."

The following is a diagram provided by the Article 29 Working Party for conducting a DPIA"



Data Breach Notification

GDPR Articles 33, 34

The GDPR imposes certain mandatory data breach reporting obligations. The GDPR defines "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Whenever the breach is likely to result in a high privacy risk for data subjects, these individuals must be notified.

Controllers must notify Supervisory Authorities and individuals without undue delay after becoming aware of a personal data breach. Where "feasible," data controllers must notify Supervisory Authorities no later than 72 hours after having become aware of a breach. Controllers do not have to report a breach in the event it is not likely that the data breach would result in a risk to the rights and freedoms of the individual.

Vendor Management

Articles 24, 28

Under Article 24, it is the responsibility of controllers to ensure that all processing of personal data complies with the GDPR. Under the GDPR Article 28, when selecting processors, controllers must make sure that the processors provide "sufficient guarantees" of their ability to comply with GDPR. Processors cannot subcontract with another processor without prior written authorization of the controller.

There must be a contract between the controller and processor. The GDPR sets forth a series of requirements for these contracts:

- the processor must process personal data only on documented instructions from the controller
- the processor must ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality
- the processor must have security safeguards as required by GDPR
- the processor must respect the rules regarding engaging another processor
- the processor must provide any assistance necessary for the controller to provide for the rights of data subjects
- the processor must assist the controller in complying with security safeguards and breach notification requirements
- the processor must delete or return all personal data to the controller at the controller's requests after the end of the processing
- the processor must provide information to the controller to demonstrate compliance and must allow for audits and inspections by the controller