The EU General Data Protection Regulation (GDPR):

What It Means for US Businesses

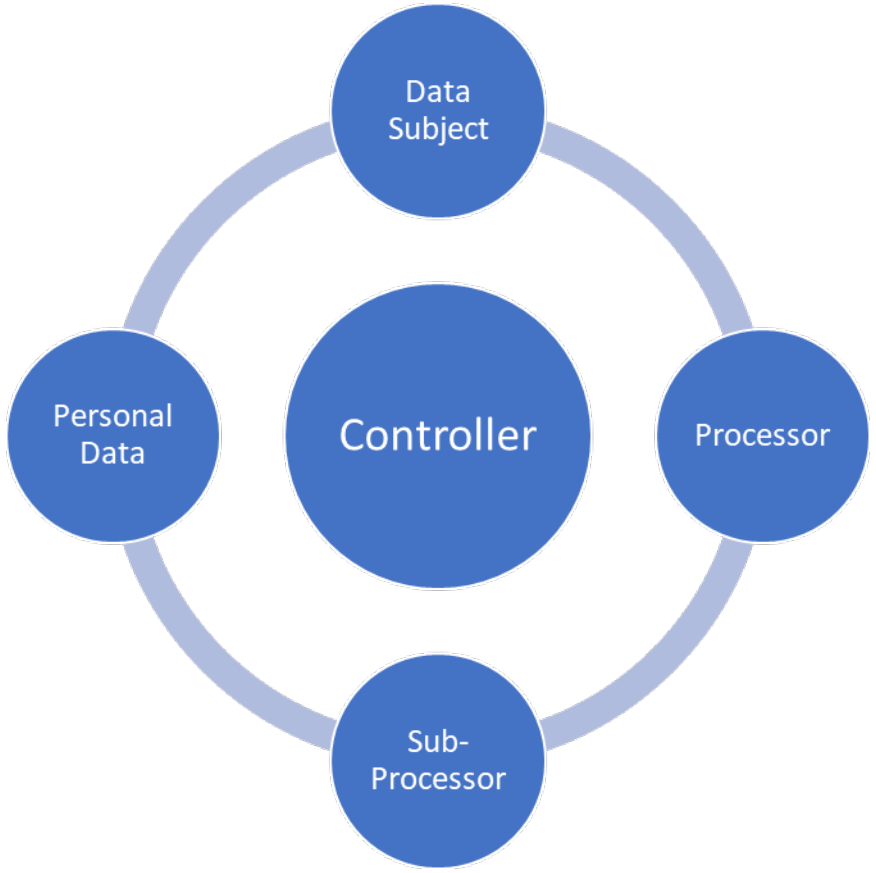
GDPR Overview and Key Terms

- Effective date: May 25, 2018
- Regulates “processing” of “personal data” of “data subjects” in the EU by “controllers” and “processors” of data
- Top potential fines: the greater of €20m or 4% of global revenues

GDPR Overview and Key Terms

- “Data subject” = a person in the EU
- “Personal data” = information sufficient to allow the identification of an individual
  - “Special categories” of sensitive personal data reveal racial/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life
- “Processing” = anything done to or with personal data, including collecting, storing, deleting

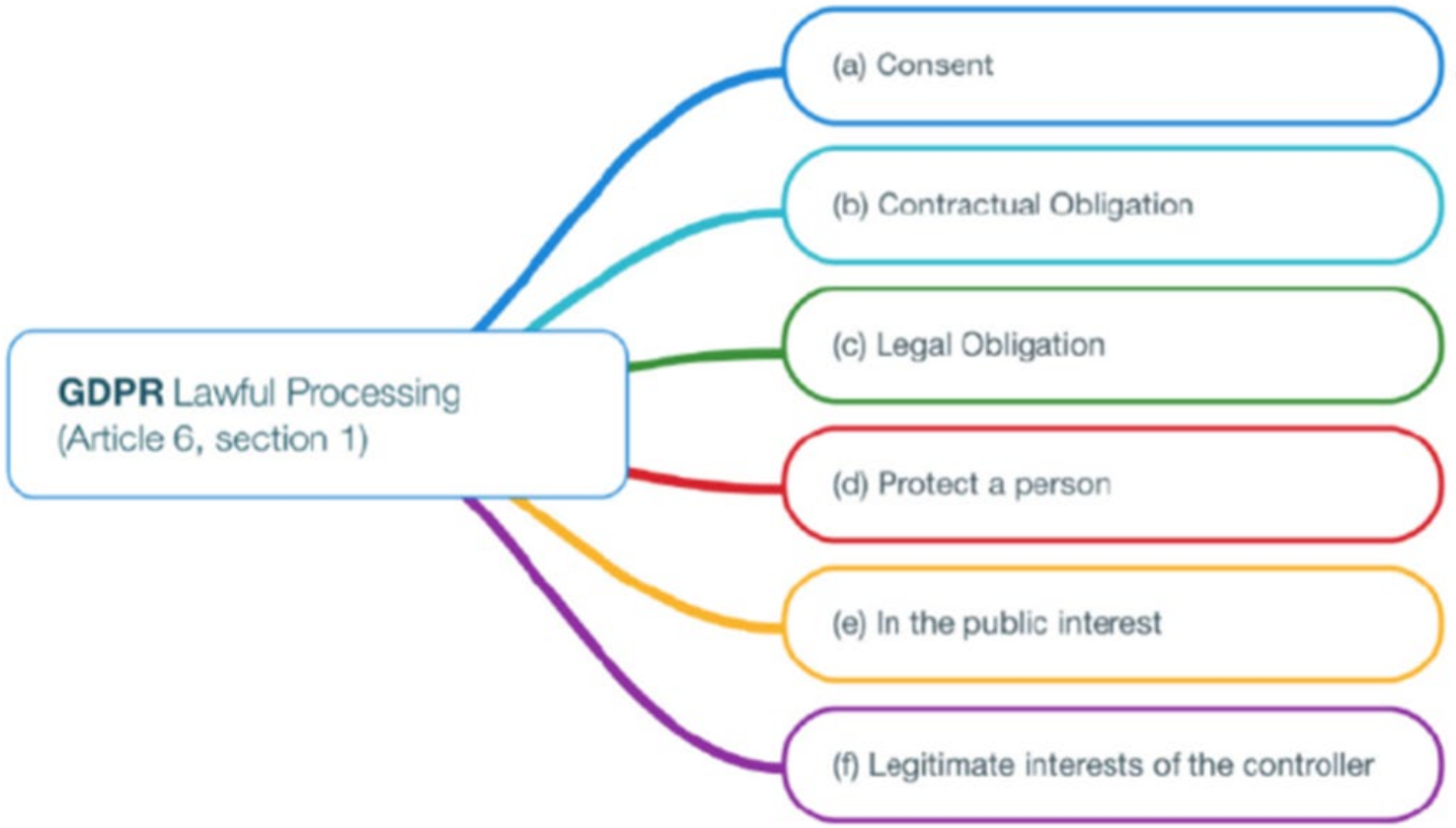
Roles and Responsibilities of Data Controllers and Processors (and Subprocessors)



Rights of Data Subjects

- **Right to Transparency**
- **Right to Access**
- **Right to Rectification**
- **Right to Restrict of Processing**
- **Right to Object**
- **Right to Data Portability**
- **Right to Be Forgotten**

Lawful Bases for Processing Personal Data



Lawful Bases for Processing Personal Data

- Article 6.1.a-f
- Consent by Data Subject for specific purpose
- Processing necessary for:
- Performance of Contract involving Data Subject
- Compliance with a legal duty of the Controller
- Protection of a vital interest, data subject or other
- Performance of public interest task or as official authority
- Legitimate interests of Controller, or 3d party, subject to fundamental rights and freedoms of data subject, esp. children
- See Recital 40

Article 6.1.a-b, Data Subject Consent and Contracts

- Consent Conditions, Article 7
- B of P on Controller to demonstrate
- Written Consent must be clear
- Notice of Right to withdraw Consent must precede giving of Consent
- Tender Subjects affecting Consent
- Child Consent- Article 8 (age 16/13, parent)
- “Special Categories” of data- Article 9- (race/politics/sex, etc.) “explicit consent”/other bases
- Criminal Convictions and Offences- Article 10
- Performance of a Contract
- Consent for extra-K processing dubious

Privacy Notices: Article 12

- Article 12 Identifies information due from the Controller to a Data Subject- obligations derive from Data Subject Rights
- The Controller actions are obligatory, require timely action
- Articles 13-14, 15-22, and 34
- 13-14- Information to be provided to the data subject when data are provided by the data subject, and when the data is obtained elsewhere- detailed contact, transfer, purpose, data source, processing information

- Privacy Notices: Articles 15-22, 34

- 15-22- Data Subject's rights of:
- Access
- Rectification and Erasure (Controller duty to broadcast)
- Restricting processing
- Data Portability
- Involvement in Automated Decision Making/Profiling
- Article 34 Notice of Data Breach

Extraterritorial Application to U.S. Entities

Article 3.1-

- GDPR applies to entities established in the Union – don't just think HQ/PP of Business

Article 3.2-

- Regulation "applies to processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
- a) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- b) The monitoring of their behavior as far as their behavior takes place within the Union.

Article 3.3-

This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Extraterritorial Application to U.S. Entities

Article 3.2.a-b

"where the processing activities are *related to*"

"The offering of goods or services"

"to such data subjects *in the Union*"

"The monitoring of their behavior as far as their behavior takes place *within the Union*"

Recitals 22 (concerning establishment); 23 (processors not established in the Union if data subjects within the Union are "targeted")

Vendor Contract Data Processing Agreements

- A challenging aspect of GDPR compliance is integrating the law's requirements into existing vendor management relationships, agreements, policies and procedures.

- Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

- Processing by a processor shall be governed by a contract or other legal act, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

DPO and EU Representative Requirements

Article 37º

- The controller and the processor shall designate a data protection officer if:

(a) the processing is carried out by a public authority or body;

(b) the core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities consist of processing on a large scale of special categories of data (eg: health data) and personal data relating to criminal convictions and offences.

DPO and EU Representative Requirements

Tasks of the data protection officer:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with GDPR and with the internal policies of the companies in relation to the protection of personal data;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority and the data subject on issues relating to processing.

Privacy by Design & IT Processes

Article 25º

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Steps to Compliance

1 - Project Governance and Assessment

2 - GAP Analysis

3 - Risk based approach

4 - Key milestones

5 - Roadmap for implementation

6 - Implementation