General Data Protection Regulation

Selected GDPR Myths

Laura De Boel

Of Counsel

Wilson Sonsini Goodrich & Rosati, LLP

June 28, 2018

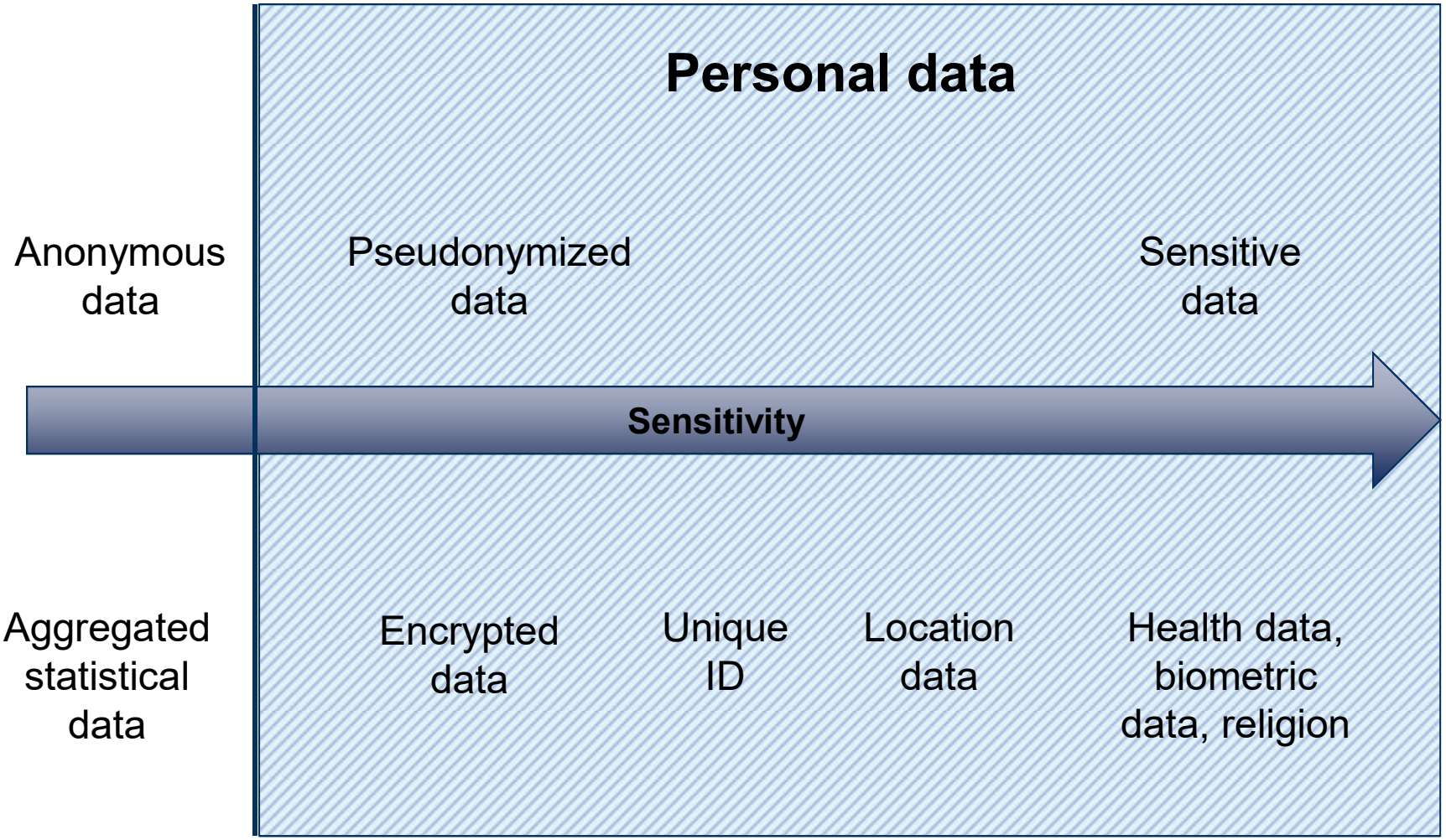
Background

- Most important piece of EU data protection legislation for next decades.
- From Directive 1995/46 to the GDPR.
  - Long review: started in 2010.
  - Directly applicable in all EU countries, but expect **local deviations**:
    - Cultural differences impacting regulators' approaches will most likely remain.
    - Some areas can be further specified by local law (e.g., Human Resources).
    - Need to modify local data protection laws.
- Very detailed legislation based on ***same core principles*** with :
  - Stricter rules and new concepts.
  - Enhanced individuals' rights.
  - Obligation to demonstrate compliance with GDPR (accountability principle).
  - Increased enforcement and fines (up to 4% of annual worldwide turnover).
- Enforceable as of May 25, 2018
- Significant buzz around GDPR; created a number of myths.

Background

Data Controller	Data Processor
The entity that, alone or jointly with others, determines: - the purposes ("why") and - the means ("how") of the data processing. Joint controllers vs. separate controllers?	The entity that processes personal data: - on behalf of and - under the instructions of the controller. Sub-processors?

Background


Personal data
Anonymous data
Pseudonymized data
Sensitive data
Sensitivity
Aggregated statistical data
Encrypted data
Unique ID
Location data
Health data, biometric data, religion

Myth 1: We don't need to comply with the GDPR as we don't have any affiliate, subsidiary, or branch in the EU.

EU companies

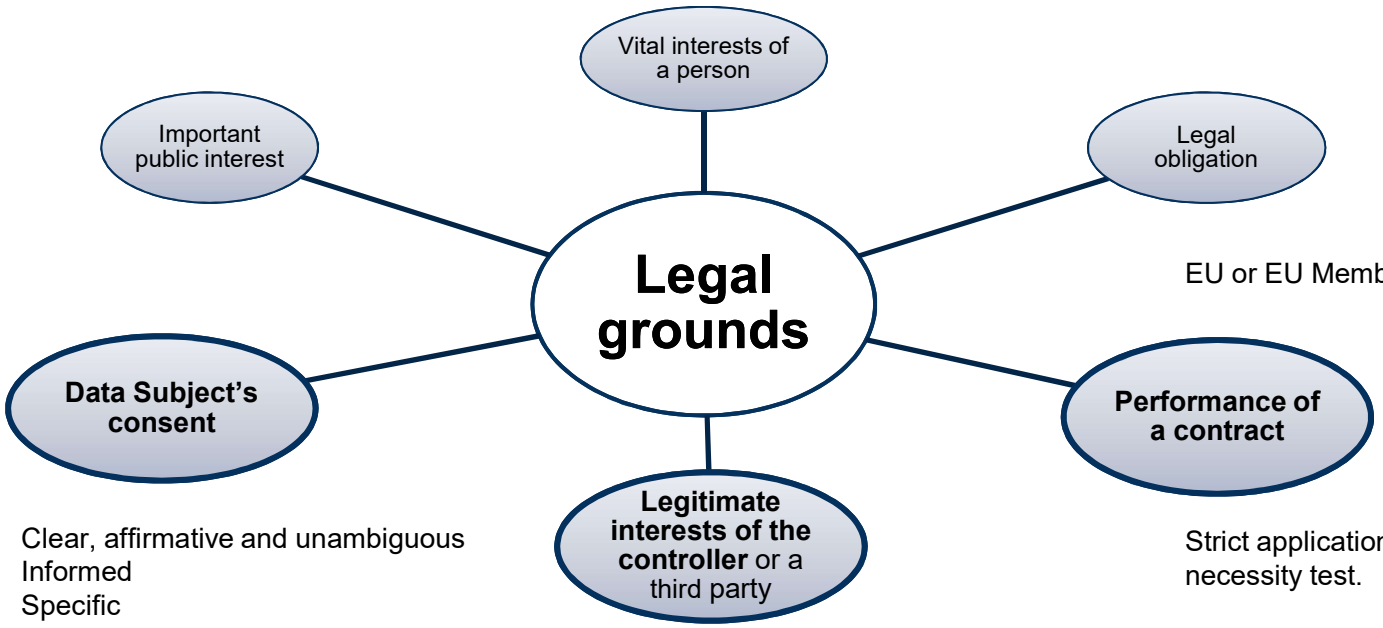
- Controllers and processors "established" in the EU.
- "Establishment" implies the effective and real exercise of activity through stable arrangements, regardless of its legal form (e.g., branch, subsidiary).

Non-EU companies

- Controllers and processors:
  - Offering of goods / services to individuals in the EU, even free of charge.
  - Monitoring the behavior of individuals located in the EU.
- "Targeting" of EU individuals?

- The GDPR does not apply in all situations.
- Incentive often comes from EU or global customers.

Myth 2: Consent is always required to process personal data



EU or EU Member State's obligation.

- Clear, affirmative and unambiguous
- Informed
- Specific
- Freely given
- Can be withdrawn.

Strict application of the necessity test.

- Reasonable expectations of individuals.
- Balancing test.
- Increased notice obligation.
- Right to opt-out from processing.
- Internal documentation.

Other legal grounds for sensitive data

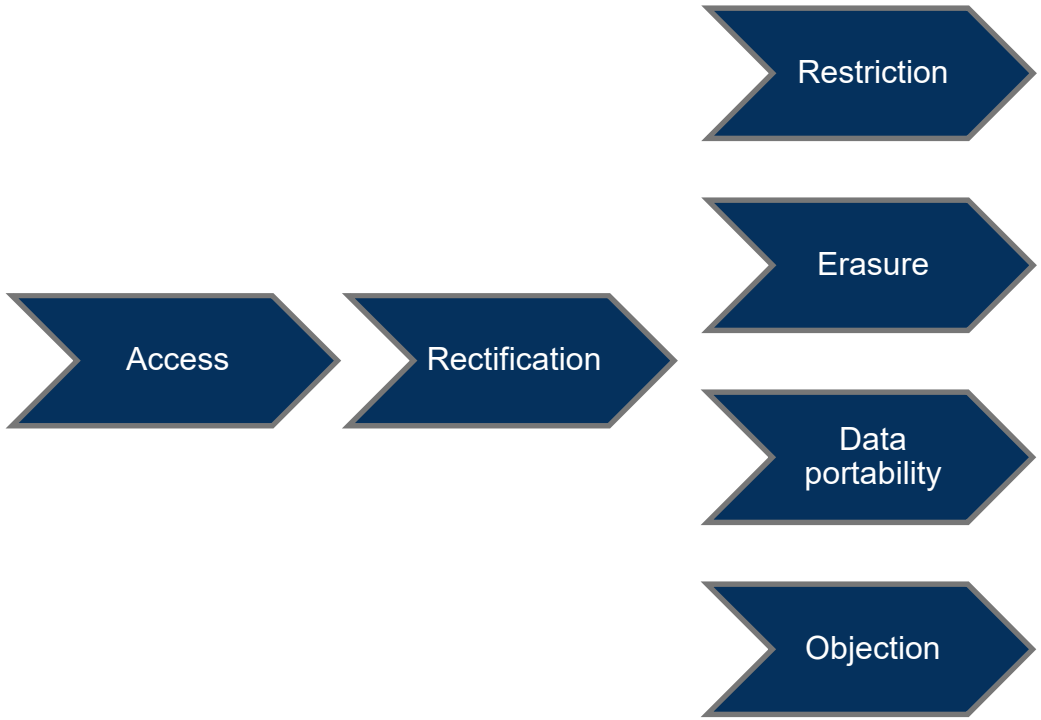
Myth 3: We must send an e-mail to our users to gather their opt-in consent for marketing

- Electronic marketing is regulated by the E-Privacy Directive (which is currently under review)
- Opt-in is required unless companies can rely on the opt-out exception:
  - Data must be collected in the context of a sale
  - Opportunity to opt-out at the time of collection and in each marketing communication
  - About similar products or services by the same legal entity
- GDPR regulates what constitutes a valid consent
- Sending an e-mail to gather consent is inappropriate in most cases

Myth 4: We must e-mail our users about the update of our privacy policy

- Privacy notice must be concise, transparent, intelligible, easily accessible, and the language should be clear and plain, especially when addressed to a child.
- GDPR significantly increases the amount of information that controller must provide to individuals (e.g., legal grounds, data retention, data transfers, disclosure).
- Layered privacy notice
- Not required to send an e-mail to individuals.
  - Material changes vs. non-material changes
  - Other means (e.g., pop-up, “new” bubble)
- Not clear template yet
- Option to use standardized icons
- Trade-off between U.S. and EU requirements

Myth 5: Data subjects rights are absolute; after all data protection is a fundamental right



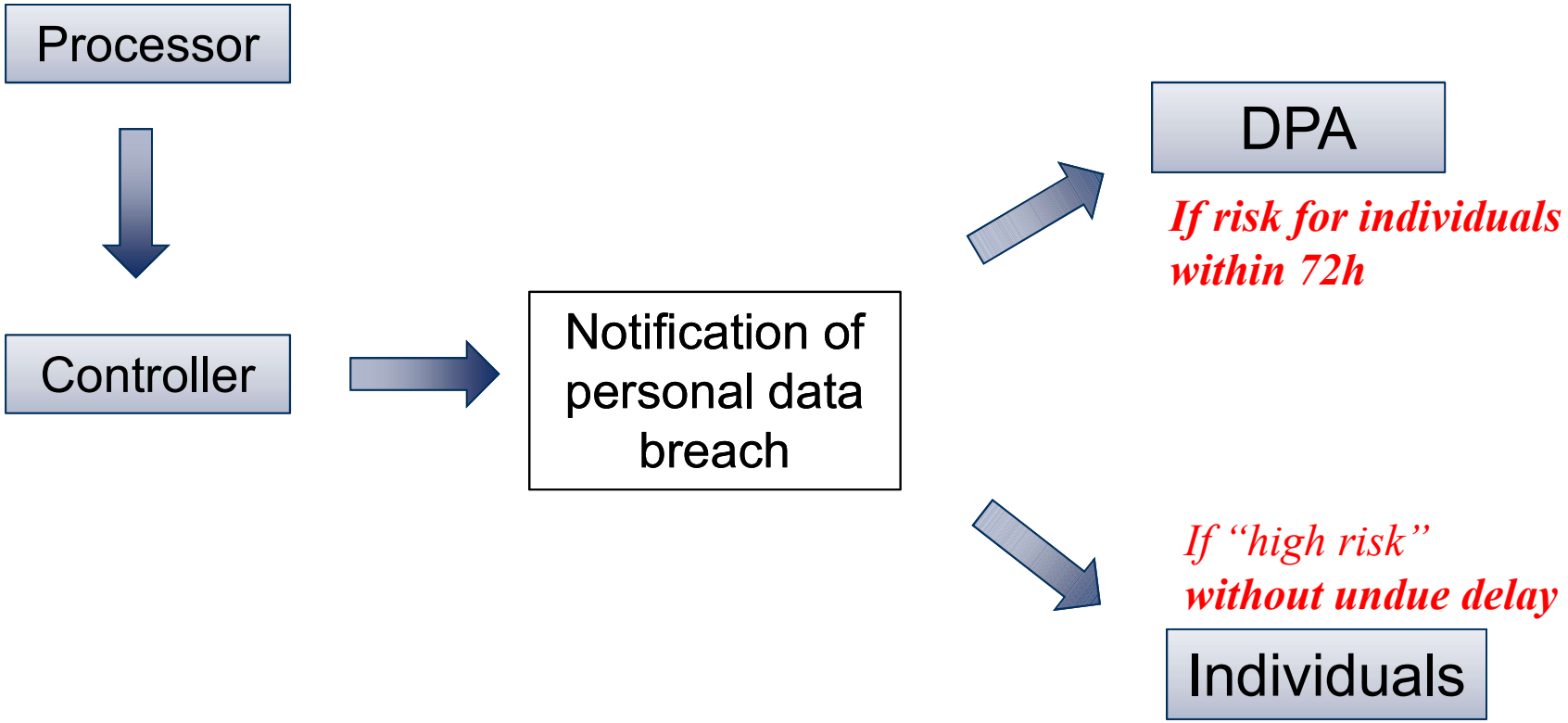
Myth 6: All companies must appoint a DPO

General rule	• Companies (controllers and processors) ***may*** appoint a DPO. • But consider appointing a DPO as a ***best practice***, but then must comply with GDPR requirements.
Mandatory appointment	• Large-scale, regular and systematic monitoring of individuals. • Processing of sensitive data and data relating to criminal convictions and offences (if company's core data processing activities). • National laws may require companies to appoint a DPO in other cases (e.g., Germany).
Tasks	• Advises company and its staff on GDPR obligations. • Monitors compliance with GDPR and internal privacy policies (e.g., assignment of responsibilities; awareness-raising; trainings; audits). • Provides advice on PIA and monitors its performance. • Cooperates with DPA and acts as its contact point (e.g., in case of DPA consultation).

Qualifications	• Expert knowledge in data protection law and practices. • Ability to fulfill his / her tasks.
Companies obligations	• Publish the DPO contact details in privacy notices and notify them to DPA. • Involve DPO in all data protection issues. • Provide DPO with resources necessary to: (1) perform his or her tasks; (2) access personal data and data processing activities; and (3) maintain his or her expert knowledge.

Position of DPO	• Strict requirement of DPO independence.
	  • May be a member of staff or a contractor but should be able to perform tasks independently.
	  • Can fulfil other tasks as long as there is no conflict of interest.
	  • Cannot receive instructions, and cannot be dismissed or penalized for performing tasks.
	  • Must directly report to the company's highest management level.
	• Is bound by confidentiality / secrecy obligation.
	• A group of companies may appoint a single DPO if easily accessible from each establishment.

Myth 7: All data breaches must be notified to Data Protection Authorities and individuals.



Myth 8: As a data processor, we don't have to conclude DPAs; our clients must

- Data processing agreements must be more detailed and include details on the processing (i.e., subject-matter, duration, nature, purposes, type of data, categories of individuals) .
- Additional contractual provisions requiring the processor to:
  - Only act on the controller's documented instructions (including data transfers).
  - Ensure that persons authorized to process data are bound by confidentiality obligation.
  - Implement appropriate security measures.
  - Only sub-process personal data with the prior specific or general authorization of the controller, and bind the sub-processor with similar obligations via a written agreement.
  - Make available to the controller information necessary to demonstrate compliance.
  - Assist the controller regarding individuals' requests, security measures, breach notification, PIA, prior consultation.
  - Allow for and contribute to audits (including inspections) conducted by the controller.
  - Return or delete data after processing (at the controller's choice).
- Possibility to use template agreements adopted by the EU Commission (not available yet).
- Joint-controllers vs. separate controllers

Myth 9: Data transfers outside of Europe are prohibited; we must store data in the EU

- Maintains existing restrictions and confirms / creates data transfer mechanisms:

Adequacy decisions	• Existing decisions valid until repealed by the EU Commission. • New set of criteria for new adequacy decisions.
Binding Corporate Rules (BCRs)	• Explicit recognition for both controllers and processors.
Standard contractual clauses (SCC)	• No DPA authorization.
Derogations	• Legitimate interests of a controller (with limitations).
New data transfer mechanisms	• Codes of conduct and certification mechanisms with binding commitments (unclear).
Conflict of laws	• Any disclosure must be based on an international treaty such as a MLAT.

An area still in turmoil:

  - Ongoing controversy over EU-U.S. Privacy Shield (replacing EU-U.S. Safe Harbor).
  - Question of validity of SCC raised before the CJEU.

- BCRs are and will be seen very favorably in the EU.

Myth 10: Data Protection Authorities will automatically fine companies

Increased judicial remedies for Individuals	• Right to lodge a complaint before a DPA. • Right to an effective judicial remedy against a DPA. • Right to an effective judicial remedy against a controller or a processor. • Right to seek compensation for damages against a controller or a processor. • Data protection associations with right to sue companies.
DPAs' investigative powers	• Conduct investigation (e.g., audit). • Notify companies in case of infringement. • **Dawn raid.**
DPAs' corrective powers	• Issue warnings or reprimands. • Order companies to comply with individuals' rights. • Order to bring the processing activities in compliance with the GDPR. • Impose a limitation on processing. • Suspend data transfers. • **Impose massive fines (up to 10 / 20 million, or 2% / 4% of global turnover).**
DPAs' authorization and advisory powers	• Prior consultation. • Advice on draft codes of conduct. • Accreditation of certification bodies. • Adoption of SCC or authorization of ad hoc contract clauses. • Approval of BCRs.

Questions?

Thank you!

Laura De Boel

Of Counsel

Wilson Sonsini Goodrich & Rosati

ldeboel@wsgr.com