GDPR (Since May 25th 2018)

Grants individuals the following rights

* Be notified within 72 hours after private data have been compromised
* Right to access data
* Right to be forgotten
* Data portability

Privacy is a fundamental right in the EU, for all EU citizens, all over the world, hence the GDPR has an extra-territorial approach.

An organization needs to

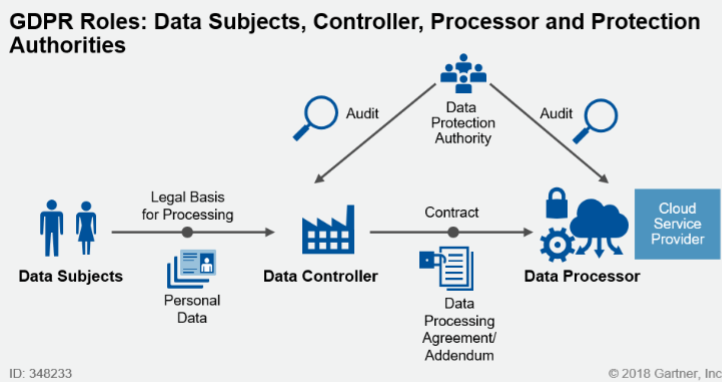
* Appoint an accountable employee
* Ensure safeguards are in place to stop attackers
* Ensure suppliers are GDPR compliant
* Ensure users are always asked to consent
* Report breaches within 72 hours
* Proof of privacy by design
* Massive penalty: Up to 4% of the worldwide annual turnover of the previous fiscal year or up to €20 million, whichever is greater

GDPR definition of private / personal data

* Data / information that relates to an identified or identifiable living individual
* Data that has been de-identified, encrypted or pseudonymised, but can be used to re-identify a person remains personal data
* Data that has ben rendered anonymous in such a way that the individual is not or no longer identifiable is not personal data anymore
* GDPR protects data regardless of the technology used for processing data

Principles that organizations storing personal data MUST follow

* Purpose limitation: have specific purpose for processing the data, must indicate those purposes to individuals when collecting their personal data, cannot reuse the personal data for other purposes that are not compatible with the original purpose
* Data minimization: collect and process only the personal data necessary to fulfil the specific purpose
* Accuracy: ensure the personal data is accurate and up-to-date, having regard to the purpose for which it is processed, and correct it if not
* Storage limitation: ensure that personal data is stored for no longer than necessary for the purposes for which it was collected
* Integrity and confidentiality: install appropriate technical and organisational safeguards that ensure the security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technology

GDPR Authorities

* Data controller: determine the purpose for which & the means by which personal data is processed
* Data processors: processes personal data on behalf of the controller
* Data protection officer: assisting controller, reports to the highest level of management of the organization

What happens when a breach has been taken place

* If it is likely that the breach poses a risk to an individual’s rights and freedom
  + Your organization has to notify the supervisory authority without undue delay, and at the latest within 72 hours after having become aware of the breach
* If you organization is a data processor
  + It must notify every data breach to the data controller
* If the data breach poses a high risk to those individuals affected
  + Those individuals should all also be informed, unless there are effective technical and organisational protection measures that have been put in place, or other measures that ensure that the risk is no longer likely to materialise
* Whenever processing is likely to result in a high risk to the rights and freedoms of individuals
  + A data protection impact assessment (DPIA), done from an authorized and certified organization, is required

Privacy by Design – principles

* Proactive not reactive
* Privacy as the default setting
* Privacy embedded into design
* Full functionality
* End-to-end security
* Visibility and transparency
* Respect for user privacy

Privacy Engineering – Development lifecycle

1. Requirements
2. Data Protection Impact Assessment
   1. Risk assessment
3. Specifications
4. Development Phase
5. Testing
6. Production
7. Service continuity (and problems)
8. End of life

PET (Privacy Enhancement Technologies)

* Encryption (Confidentiality, Integrity, Nonrepudiation)
  + Public key Cryptography
  + Symmetric Cryptography still has a place
  + Hashing
* Access control
  + Granularity of access control level: Collection level / Record level / Cell level / Metadata
  + Federated systems, federated access control
  + Multi-factor authentication
* Anonymisation / Pseudonymisation
  + Anonymisation
    - Cannot be used to identifying a natural person
      * “Mark spent 30€ on a bottle of Scotch” 🡪 “A customer spent 30€ on an item”
    - Difficult for “Big Data”, because issues with linking
  + Pseudonymisation
    - Replacing attributes to anonymise natural persons that might be reversable
      * “Mark spent 30€ on a bottle of Scotch” 🡪 “Customer x spent 30€ on item 56152”
    - No reason to not use it