The role of controller within GDPR

.I Definition

The controller is actually **in charge of processing definition framework**: (s) he "*determines the purposes and means of the processing of personal data"* so (s) he is the contact person and the contracting party with the data subject.

The controller can be "*the natural or legal person, public authority, agency or other body* […] alone or jointly with others".

Where Union or Member state law determines the processing, the controller must be eligible according to *the specific criteria for its nomination […] provided for by Union or Member State law;"*[1]

.II Responsibility of the controller

- Implement appropriate technical and organisational measures.
  - ➔ Pseudonymisation: user as ID and not with real contact details
  - ➔ Data minimisation: only data required for processing
- Implement appropriate data protection policies.
- Adhere to approved code of conducts or approved certification mechanisms

CSQ 1? Burden of proof: the controller must demonstrate that the processing is performed in accordance and compliance with this Regulation

Examples:

- *Review terms and condition for user, put it online using a pop-up: when the user connects, allow connection only if user read the text.*
- *Contact users/customers with e-mail about new data policy*
- *Inform users/customers with article in newsletter or mailshot when they have subscribed: the next time they connects , they must review terms and conditions before going ahead using application (web site, mobile applications or e-services)*

CSQ 2? Joint controllers: when two or more controllers determine jointly the purposes and means of processing, they have to define their arrangements or gentleman agreements

.III Duties

1. Information and communication

Whom?

- Data subject
- Processor(s), joint controller(s)
- supervising authority

[1] See point (7), http://eur-lex.europa.eu/legal- content/EN-FR/TXT/?uri=CELEX:32016R0679&fromTab=ALL&from=EN

When?
- Before processing
- request from data subject (*e.g. access, erasure, rectification*)
- infringement by another controller to supervising authority

What?
- Legal notice about processing
- Disclaimer about data privacy
- Mailshot to customers/users
- Notification of breach
- Allowance for consent

2. Maintain a **record of processing** activities

When?
- Companies /organisation with at least **250 employees**
- Risk to the **rights of freedoms of data subjects**, not occasional or including specific categories of data

What?
- contact details of controller(s) and its representatives or DPO
- purposes of processing
- categories of data subjects and personal data
- transfer of personal data to a third country or an international organisation (**e.g. Passenger Name Record**)
- erasure (period/time/limits)
- Security measures:
  - ➔ Pseudonymisation (e.g. user connect as ID or using session ID)
  - ➔ ensure confidentiality, integrity , availability and resilience of processing system and service (e.g. information in terms and conditions, restriction of device by tick box in mobile app)
  - ➔ restore availability and or access to personal data (e.g. retrieve data when asking questions to log in)
  - ➔ testing procedure before updates or releases
  - ➔ risk assessment of processing activities (**e.g. SWOT, amdec**)
  - ➔ Adherence to approved code of conducts or approved certification mechanisms
  - ➔ Responsibility (see art 1384 cciv[2], be, fr, lu)

2. Cooperation with the supervisory authority (e.g. CNPD, CNIL)
   - Notification of a personal data breach within 72 hrs. after having become aware
   - Communicate breach to data subject

3. Impact assessment

When?
- Use of new technology and risk to rights and freedoms of natural persons
- Systematic and extensive evaluation of personal aspect including

[2] *Art 1384 al 2 ,CCIV : « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde.[…] Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés; »*

profiling

- A large scale data from special categories[3] (e.g. racial or ethnic, genetic, biometric, religious, membership, labour law, person with disabilities and so on) or relating to criminal convictions (e.g. criminal record)
- Example: Some public or private employers require a copy of criminal record as condition for employment contract.
- A systematic monitoring of a public accessible area
- Example: telephone number or contact details from public directory

What?

- Description of processing operations + purposes + legitimate interest pursued by controller
- Assessment of necessity and proportionality (= need and requirements of processing)
- Risk assessment
- # the rights and freedoms of natural persons (= risk identification)
- # precaution, security measures
- Respect of codes of conducts

Who?

- Supervising authority : establish a list of processing operations for which such impact assessment is mandatory or not regarding the consistency mechanism
- activities related to goods or services offers : e-commerce, real estate
- behaviour monitoring in several members stats : marketing issues
- free movement of personal data : cloud services, merge and acquisitions
- Data subject: views about some processing: e-mail to inform the consequences of such processing and if the data subject is agree to carry on.
- Controller : assess if processing is performed in accordance (= Quality control and Quality insurance)

4. Prior consultation

When?

- An impact assessment is required AND the risk is too high if any measures are not taken
- The supervising authority thinks the processing would infringe the Regulation: the controller receives within 8 weeks an advice to improve the request. It could be extended to 6 weeks.
- Requirement from member's states in the public interest, social protection and public health (e.g. data processing of patient in clinical trial)
-

What?

- Respective responsibilities of stakeholders (= controller(s), processor(s), third parties)

[3] See art 9 , http://eur-lex.europa.eu/legal-content/EN-FR/TXT/?uri=CELEX:32016R0679&from=EN

- Definitions of purposes and means
- Measures and safeguards
- Contact details of DPO
- Data Impact assessment
- Any other required information

Who? Contact the supervising authority