

In response to your enquiry, I am presenting a brief description of most important data protection rules in the General Data Protection Regulation and short guide on the processing of personal data.

Step 1 - determine whether the GDPR is applicable

Material scope

- Art 2 (1) whether the company is **processing** (wholly or partly) by automated means by definition art 4(2)) **personal data** (definition art 4 (1)).
- Art 2 (2) whether some of the exceptions are applicable.

Territorial scope

- Art 3 (1) in the context of the activities of an **establishment (the branch) of a controller** (responsibility, determines the purposes and means, definition art 4 (7)) **or a processor** (definition art 4 (8)) **in EU**.
- Art 3 (2) personal data subjects are in EU, data controller or processor not in EU, but **processing activities are related** to the offering of goods or services **to data subjects** or the monitoring of their behavior **in EU**.

Step 2 - determine whether the processing of the data complies with seven key principles in art 5 GDPR

- Art 5 (1) (a) **lawfulness, fairness and transparency** in relation to the data subject.
- Art 5 (1) (b) **purpose limitation**, specified and legitimate purposes, compatible with the initial purposes.
- Art 5 (1) (c) **data minimization**, relevant and limited data, necessary in relation to the purposes.
- Art 5 (1) (d) **accuracy**, kept up to date data (art 16).
- Art 5 (1) (e) **storage limitation**, no longer kept than is necessary for the stated purposes.
- Art 5 (1) (f) **integrity and confidentiality**, appropriate security (art 32).
- Art 5 (2) **accountability** – responsibly for controller demonstrate compliance with principles.

Step 3 - determine whether there is lawful basis for processing of the personal data

Under art 6 specific cases of lawful basis for general processing of personal data:

- Art 6 (1) (a) genuine consent (definition art 4 (11), specific conditions art 7);
- Art 6 (1) (b) processing is necessary for the performance of a contract with the data subject;
- Art 6 (1) (c) necessary for compliance with a legal obligation;
- Art 6 (1) (d) necessary for somebody's vital interests;
- Art 6 (1) (e) necessary in the exercise of official authority, a specific task in the public interest;
- Art 6 (1) (f) necessary to achieve legitimate interests, balance it against the individual's interests, reasonably expect.

Art 9 (1) Processing of special category data (sensitive data) is allowed only if satisfy a specific condition under art 9 (2).

Art 10 Processing of personal data relating to criminal offence data can be carried out only under the control of official authority or in cases specified in national law – in Sweden according to data protection law and Swedish Data Protection Authority's (SDPA) praxis.

Art 86 Processing of the national identification number can be carried out according to specific conditions in the national law - in Sweden data protection law and SDPA's praxis.

International transfers of personal data (Chapter V) – to a third country, outside of the EEA, only if adequate levels of data protection can be ensured. More options under art 46, 47 - appropriate contractual clauses, binding corporate rules etc.

Step 4 Determine if appropriate measures are taken to provide relevant information to the data subjects (art 12, 13, 14). Ensure compliance with the rights of the data subject (chapter III).

Step 5 Determine if the personal data is processed securely, appropriate technical and organizational measures are taken to ensure security (art 25, 32). Observe other obligations of the controller.