Basics of GDPR

1. Definition of Personal Data and Processing
2. Six Principles of Data Processing
3. Requirements of Processing
4. Provision of Information when Data Collected
5. Rights of Data Subject (User)
6. Obligations of Controller (You/Institution)

1. DEFINITIONS OF PERSONAL DATA AND PROCESSING

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the *physical, physiological, genetic, mental, economic, cultural or social identity* of that natural person.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. SIX PRINCIPLES OF DATA PROCESSING[1]

I. **Lawfulness, Fairness and Transparency**

Data processed lawfully, fairly and in a transparent manner in relation to the data subject.

II. **Purpose Limitation**

Data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[2]

III. **Data minimisation**

Data adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

IV. **Accuracy**

Data accurate and, where necessary, kept up to date; inaccurate personal data are to be erased or rectified without delay.

V. **Storage limitation**

[1] The controller shall be responsible for, and be able to demonstrate compliance with the 6 principles ACCOUNTABILITY PRINCIPLE

[2] further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes

Data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.[3]

VI. **Integrity and Confidentiality**

Data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

[3] personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject

3. REQUIREMENTS FOR PROCESSING

I. Lawfulness of Processing [4]

1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given *consent* to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the *performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for *compliance with a legal obligation* to which the controller is subject;

(d) processing is necessary in order to *protect the vital interests* of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the p*ublic interest* or in the exercise of official authority vested in the controller;

(f) processing is necessary for the *purposes of the legitimate interests* pursued by the controller or by a third party.[5]

II. Conditions for Consent [6]

Controller has to be able to demonstrate consent.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is *clearly distinguishable* from the other matters, in an *intelligible and easily accessible form, using clear and plain language*. [7]

The data subject shall have the *right to withdraw* their consent at *any time*.

[4] Article 6
[5] except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
[6] Article 7
[7] Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

III. Prohibition on Processing of Special Categories of Personal Data[8]

1. Processing of personal data:

revealing racial or ethnic origin,

political opinions,

religious or philosophical beliefs,

or trade union membership,

and

the processing of genetic data,

biometric data for the purpose of uniquely identifying a natural person,

data concerning health or data concerning a natural person's sex life or sexual orientation

shall be ***prohibited***.

2. (Some) Exceptions to the Prohibition:

(a) the data subject has given *explicit consent* to the processing of those personal data for one or more specified purposes. [9]

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

(c) vital interest

(d) In course of legitimate activities by foundation, association or any other non-profit body with political, philosophical, religious or trade union aim.

(e) defence of legal claims

(f) necessary for reasons of substantial public interest.

[8] Article 9

[9] except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

4. INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE COLLECTED (FROM THE DATA SUBJECT) [10]

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.[11]

[10] Article 13
[11] 46. Appropriate Safeguards
47. Binding Corporate rules

49(1) Derogations to above Articles

5. THE RIGHTS OF DATA SUBJECTS

1. Right of Access and Right to Rectification[12]

2. Right to Object and Right to Restriction of Processing [13]

3. Right to Erasure and Right to Data Portability [14]

The right to erasure (also known as “the right to be forgotten”). it allows data subjects to obtain from data controllers the erasure of personal data concerning them without undue delay.

Data subjects also have the right to data portability or, in other words, the right to receive from controllers personal data concerning them in a structured, commonly used and machine-readable format and to transmit these data to other controllers.

4. Rights regarding automated decision-making. [15]

The right not to be subjected to a decision that is based only on an automated processing, including profiling. This right is applicable when such a decision has legal consequences for an individual or in a similar manner significantly affects him or her.

[12] Article 15 & 16
[13] Article 21 & 18

[14] Article 17 & 20
[15] Article 22

OTHER RIGHTS:

5. Right to Representation and Compensation

Using another right found in Article 80 GDPR, data subjects can allow not-for-profit bodies, organisations or associations **to act on their behalf** by lodging complaints, receiving compensation and exercising some rights with regard to complaints and judicial remedies.

Finally, if individuals have suffered material or non-material damage as a result of an infringement of the GDPR they entitled to **the right to receive compensation** from the controller or processor, as stressed in Article 82 GDPR.

6. Rights concerning Complaints and Judicial Remedies

Under **Article 77 GDPR**, data subjects have the **right to lodge a complaint with a supervisory authority** in the Member States where they live and work and places of alleged infringements if they think that the processing of their personal data infringes the GDPR. It means that if our personal data are processed by a person or entity in a way that is incompatible with the regulation, a complaint can be lodged about this with a supervisory authority.

There is also **a right to an effective judicial remedy against decisions of supervisory authorities** found **in Article 78 GDPR** that is granted to natural and legal persons**.**

Furthermore, we should mention **the right to an effective judicial remedy against a controller or processor** laid down in Article 79 GDPR.

6. CONTROLLER'S OBLIGATIONS[16]

Controllers' Obligations may include:

• To maintain records of all processing activities (Article 30 GDPR);

• To cooperate and consult with supervisory authorities (Article 31 GDPR);

• To ensure a level of security (Article 32 GDPR);

• To notify the supervisory authorities and the concerned data subject in the event of a data breach (Article 33 GDPR);[17]

• To conduct a data protection impact assessment (Article 35 GDPR);

• To appoint a data protection officer (Article 37 GDPR);

• Specific obligations as regards transfer of data outside the EU (Chapter V GDPR);

• To assist data subjects with exercising their rights to privacy and data protection (Chapter III GDPR).

[16] Article 24 provides that controllers have to take **appropriate organisational and technical measures** to protect data subjects and their rights.

[17] Notification of the supervisory authority
When a data breach occurs, a controller has the obligation under Article 33 to notify the competent supervisory authority within 72 hours after becoming aware of the data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Notification of the data subject
Furthermore, the controller has the obligation to communicate without undue delay the personal data breach to the data subject under Article 34 if the breach is likely to result in a high risk to the rights and freedoms of natural persons.