EUROPEAN ASSOCIATION OF REAL ESTATE PROFESSIONS

CEPI

A guide to the General Data Protection Regulation (GDPR)

What is the GDPR?

The **GDPR** :

- Updates and modernises the rules on data protection in the EU.
- Applies the same rules to all companies offering services in the EU.
- Gives individuals new and stronger rights.
- Increases fines and sanctions.

As a regulation it applies directly in all EU Member States as from **25 May 2018**. But - Member States still have to amend their existing laws and make some adjustments in their implementing legislation so it needs to be read with the national law in each country.

What does it cover? - Articles 1 and 2

The **GDPR**:

- Covers **natural persons** with regard to the processing of personal data.
- Protects the fundamental rights of natural persons and in particular their right to the protection of **personal data**.
- Applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system (unless done in the course of a personal or household activity).

What is data processing? - Article 4

- **Personal data** means any information relating to an identified or identifiable natural person (e.g. identified by name, identification number, location data, online identifier etc.).
- **Processing** means any operation performed on personal data whether or not by automated means.
- **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate, analyse or predict aspects relating to a natural person (economic situation, preferences, interests etc.).

What principles apply to the processing of personal data? - Article 5

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to the purposes.
- Accurate and kept up to date.
- Kept no longer than is necessary for the purposes for which the data is processed.
- Processed in a manner that ensures security of the data.

The data controller (the natural or legal person who determines the purposes and means of the processing of personal data) is accountable for compliance with these principles.

When is processing lawful? - Article 6

Only when (**at least one** of) the following applies:

- The data subject has given consent.
- It is necessary for:
  - the performance of a contract;
  - compliance with a legal obligation on the controller;
  - to protect the vital interests of the data subject or of another natural person;
  - for the performance of a task carried out in the public interest;
  - for the purposes of the legitimate interests pursued by the controller or by a third party.

Member States may adapt these rules and set more specific requirements for processing.

What are the conditions for consent? - Article 7

- The controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.
- If the consent is given in a written declaration which also concerns other matters the request for consent must be distinguishable, accessible and use clear and plain language.
- The data subject can withdraw consent at any time (and must be informed of this right).
- To assess whether consent is freely given, account will be taken of whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Special categories of data - Article 9

The processing of personal data revealing racial or ethnic origin, religious beliefs, unique biometric data etc. is prohibited unless **at least one** of a number of conditions apply such as:

- The data subject has given explicit consent.
- Processing is necessary to carry out obligations and rights in the field of employment, social security and social protection law.
- Processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is unable to give consent.
- Processing relates to personal data manifestly made public by the data subject.

Rights of the data subject - Article 12

- The controller shall provide information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- The information shall be in writing, or other means including (where appropriate) electronic means. It may be provided orally (at the request of the data subject) provided that the identity of the data subject is proven by other means.
- The controller shall supply information on action taken on a request relating to the data subject's rights within one month of receipt of a request. If no action is taken the controller must inform the data subject within one month of the reasons and on the possibility of lodging a complaint and seeking judicial remedy.

Rights of the data subject - Article 13

When personal data is collected from the data subject the controller must provide information including:

- The identity and contact details of the controller; contact details of any data protection officer; the purposes of the processing; any recipients of the data; any intention to transfer the data.
- The period for which the data will be stored; the right to request access to, rectification or erasure of data, restriction of processing and the right to data portability; the right to lodge a complaint with a supervisory authority; details of the requirement or obligation to supply the data and possible consequences of failure to do so; the existence of automated decision-making including profiling.
- If the controller intends to process personal data for another purpose the data subject must first be informed.

Rights of the data subject - Article 14

Where personal data has not been obtained from the data subject the controller shall provide information including:

- The identity and contact details of the controller; the contact details of any data protection officer; the purposes of the processing and its legal basis; the categories of personal data concerned, any recipients of the personal data.
- In addition the controller shall provide information including the period for which the data will be stored; the right to request access to and rectification or erasure of data; the right to lodge a complaint with a supervisory authority; from which source the data originates; the existence of automated decision-making including profiling.

Rights of the data subject - Article 15

The data subject has the right to obtain from the controller confirmation as to whether or not his/her personal data is being processed, and if so access to the personal data and the following information:

- The purposes of the processing; the categories of data; the recipients; the period for which the data will be stored (where possible) or the criteria used to determine it; the right to request rectification or erasure of data or restriction of or objection to processing; the right to lodge a complaint with a supervisory authority; where data is not collected from the data subject any available information about its source; the existence of automated decision-making including profiling.

The controller shall provide a copy of the data being processed.

Rights of the data subject - Articles 16 and 17

- **Right to rectification** of inaccurate data without undue delay.
- **Right to erasure** ("forgotten") where (one of) the following applies:
  - The personal data is no longer necessary for the purposes for which it was collected; the data subject withdraws consent or objects to the processing (and there are no overriding legitimate grounds); the personal data has been unlawfully processed or has to be erased for compliance with a legal obligation.

  Unless the processing is necessary for reasons including:
  - The exercise of the right of freedom of expression and information; for compliance with a legal obligation or task carried out in the public interest; the establishment, exercise or defense of legal claims.

Rights of the data subject - Articles 18, 19 and 20

- **Right to restriction** of processing if one of the following applies:
  - The accuracy of the data is contested by the data subject; the processing is unlawful; the controller no longer needs the data for processing but it is required by the data subject for legal claims; the data subject has objected to processing pending verification whether legitimate grounds of the controller prevail.
- The controller shall notify any rectification or erasure of personal data or restriction of processing to each recipient of the data (unless this is impossible or the effort is disproportionate).
- **Right to data portability** for the data subject who has the right to receive data provided to a controller in a structured, commonly used and machine-readable format.

Rights of the data subject - Articles 21 and 22

- **Right to object** at any time to processing of data based on public interest or the legitimate interest of the controller (unless legitimate grounds override the rights of the data subject).
- Where personal data is processed for direct marketing purposes the data subject has the right to object at any time (including profiling so far as it is related to direct marketing).
- At the time of the first communication with the data subject (at the latest) these rights must be brought to the attention of the data subject and presented clearly.

Responsibility of the data controller - Articles 24 to 26

- The controller shall implement appropriate technical and organizational measures to ensure and demonstrate that processing complies with this Regulation.
- Adherence to approved codes of conduct or certification mechanisms may be used to demonstrate compliance.
- Appropriate technical and organizational measures must be implemented to ensure that, by default, only personal data necessary for each specific purpose of the processing is processed.
- Where two or more controllers jointly determine the purposes and means of processing they shall be joint controllers and determine in a transparent manner their respective responsibilities.

Processing - Articles 28 to 29

- The controller shall use only processors providing sufficient guarantees to implement measures so that processing will meet the requirements of the Regulation and by contract.
- The processor shall not process data except on instructions from the controller (unless required to do so by law).
- *Each controller shall maintain a record in writing containing the following:*
  - *The name and contact details of the controller; the purposes of the processing, a description of the categories of data subjects and personal data; categories of recipients to whom personal data has or will be disclosed; transfers of data and envisaged time limits (where applicable) and a general description of technical and organizational security measures.*

Records - Article 30

- *Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller containing:*
  - *The name and contact details of the processor and of each controller; the categories of processing; transfers of personal data (where applicable) and a general description of technical and organizational security measures (where possible).*
- The obligations shown in *italics* do not apply to an enterprise or organization employing **fewer than 250 persons** unless the processing is likely to risk the rights and freedoms of data subjects, the processing is not occasional or includes special categories of data or data relating to criminal convictions.

Security of personal data - Articles 32 to 34

- The controller and processor shall implement risk appropriate technical and organizational measures including:
  - The pseudonymisation and encryption of personal data; the ability to ensure confidentiality, integrity, availability and resilience of processing systems and services and to restore access in the event of an incident; a process for testing, assessing and evaluating security measures.
- In the case of a data breach the controller must notify the supervisory authority within 72 hours after becoming aware of it.
- The processor must notify the controller of any breach without undue delay.
- Where there is a high risk the controller must communicate the data breach to the data subject without undue delay.

Data protection impact assessment - Article 35

- Where a type of processing is likely to result in high risk to the rights and freedoms of natural persons the controller shall (prior to processing) carry out an assessment of the impact on the protection of personal data.
- The supervisory authority shall publish lists of the kind of processing activities for which an impact assessment is/is not required.
- The assessment must contain:
  - A systematic description of the processing and purposes; an assessment of the necessity and proportionality in relation to the purposes and the risks to the rights and freedoms of the data subjects; the measures envisaged to address the risks.

Data protection officer - Articles 37 and 38

- The controller and processor shall designate a data protection officer in any case where:
  - The processing is carried out by a public authority or body; the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or involve on a large scale special categories of data.
  - Or in other cases where they choose or are required by law to designate a data protection officer.
- The controller and processor shall ensure that the data protection officer is involved in all issues relating to the protection of personal data.

Tasks of the data protection officer - Article 39

- The data protection officer shall have at least the following tasks:
  - To inform and advise the controller or the processor and employees; to monitor compliance with this Regulation and policies including assignment of responsibilities and training of staff; to provide advice where requested as regards the data protection impact assessment; to cooperate with the supervisory authority and act as the contact point on issues relating to processing.
- In performing these tasks the data protection officer shall have due regard to the risk associated with processing operations.

Codes of conduct - Article 40

- The Member States, supervisory authorities, European Data Protection Board and Commission shall encourage codes of conduct to contribute to the application of the Regulation.
- Associations and other bodies may prepare codes of conduct with regard to:
  - Fair and transparent processing; legitimate interests pursued by controllers in specific contexts; collection of personal data; pseudonymisation of personal data; information provided to the public and to data subjects; exercise of the rights of data subjects; information to and the protection of children; measures and procedures; notification of personal data breaches, transfer of personal data; out-of-court proceedings and other dispute resolution procedures.

Codes of conduct - Article 40

- Associations which intend to prepare a code of conduct shall submit a draft to the supervisory authority which will give an opinion on whether it complies with this Regulation and approve it if it provides sufficient appropriate safeguards.
- The Commission may, by way of implementing act, decide that the approved code of conduct has general validity within the EU.
- All approved codes will be collected in a register and made publicly available.

Monitoring of approved codes of conduct - Article 41

- The monitoring of compliance with a code of conduct may be carried out by a body which is accredited for that purpose by the competent supervisory authority which has:
  - Demonstrated its independence and expertise; established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, monitor their compliance and review its operation; established procedures and structures to handle complaints which are transparent to data subjects and the public and demonstrated to the satisfaction of the competent authority that its tasks and duties do not result in a conflict of interests.
- An accredited body shall take appropriate action in cases of infringement of the code including suspension or exclusion.

Certification - Article 42

- The Member States, the supervisory authorities, the European Data Protection Board and Commission shall encourage (in particular at EU level) the establishment of data protection certification mechanisms and of data protection seals and marks to demonstrate compliance with this Regulation.
- Certification must be voluntary and available via a transparent process.
- Certification does not reduce the responsibility of the controller or the processor for compliance with this Regulation and will be for a maximum of three years (renewable).

Certification bodies - Article 43

- Certification will be issued by certification bodies which have an appropriate level of expertise in data protection and are accredited by one or both of the supervisory authority and the national accreditation body.
- Certification bodies will be accredited only when they have:
  - Demonstrated their independence and expertise in relation to the subject-matter; undertaken to respect the relevant criteria; established procedures for the issuing, review and withdrawal of the certification, seals and marks; established transparent complaint procedures; and demonstrated that their tasks and duties do not result in a conflict of interests.

Remedies - Articles 77 to 82

- Every data subject has the right to:
  - Lodge a complaint with a supervisory authority.
  - An effective judicial remedy against a supervisory authority.
  - An effective judicial remedy against a controller or processor.
  - Compensation from the controller or processor (who are both liable unless able to prove that they are in no way responsible for the event giving rise to the damage) for material or non-material damage, each of whom is liable for the entire damage.

Fines and penalties - Articles 83 and 84

- The supervisory authority has the right to impose administrative fines (as well as sanctions) taking into account:
  - The nature, gravity and duration of the infringement; its intentional or negligent character, any action taken to mitigate the damage; the degree of responsibility of the controller or processor; any previous infringements; degree of cooperation, categories of personal data affected; the manner in which it became known (and who notified); previous sanctions, adherence to approved codes of conduct or certification schemes; any other aggravating or mitigating factor.
- Infringements may be subject to fines up to 10 000 000 EUR or up to 2% of the total worldwide annual turnover of an undertaking for the preceding financial year whichever is the higher.

Fines and penalties - Articles 83 and 84

- Infringements can attract fines of up to 20 000 000 EUR or up to 4% of the total worldwide annual turnover of an undertaking for the preceding financial year (whichever is higher) for certain provisions including:
  - The basic principles for processing; the data subjects' rights, specific obligations adopted by Member States and non-compliance with an order or limitation on processing by the supervisory authority.
- Member States determine the rules on other penalties for infringements not subject to administrative fines and must notify these to the Commission by 25 May 2018.

Specific processing situations - Articles 85 to 91

- Member States shall determine provisions relating to specific situations including:
  - The right to freedom of expression and information; processing of the national identification number; processing in the context of employment to provide for more specific rules to ensure the protection of employees' personal data including suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights with regard to the transparency of processing and the transfer of personal data within a group of undertakings or enterprises; rules respecting obligations of secrecy where necessary and proportionate to reconcile them with the right of protection of personal data.

References and sources of help

European Commission online tool on data protection

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

European Data Protection Supervisor

Https://edps.europa.eu/

Text of the GDPR

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

CEPI aisbl,Brussels February 2018