Level 1

Main notions and fundamental principles of the GDPR

Key words: consent - controller - data processor – DPO - GDPR - legal basis - opt-out - personal data - purpose - right of access - right to erasure - right to object

Luxembourg House of Cybersecurity

CNPD National Commission for Data Protection Grand-Duchy of Luxembourg

Co-funded by the European Union

Update : 4th June 2024

THE ACTORS OF THE GDPR

The National Commission for Data Protection (CNPD)

In Luxembourg, the CNPD is responsible for verifying the legality of files and all collection, use and transmission of data concerning identifiable individuals.

In this context, it must ensure respect for the fundamental rights and freedoms of natural persons, in particular their privacy.

Data subject

Any natural person who is subject to the processing of personal data.

Controller

Any body that determines the purposes and means of the processing of personal data.

This can be an administration, a company, an association, a professional or a self-employed person.

Processor

Any body that processes personal data on behalf of and at the direction of the controller.

Data Protection Officer

See factsheet No 13

HOME THE "BASICS"

1. GDPR, General Data Protection Regulation

Date of application

25th May 2018

Objectives (non-exhaustive):

- Giving individuals control over their personal data;
- Ask companies managing data to:

» Justify the collection, processing and storage of personal data;

» Ensure their integrity, availability, security and confidentiality;

» Inform data subjects about their rights (modification, deletion, data portability, etc.); and

» Appoint a data protection officer in certain cases.

Am I concerned?

As soon as your organisation collects and processes personal data and is established on the territory of the European Union, your organisation is subject to the GDPR, regardless of its size, legal form, activities or corporate purpose.

The GDPR applies to:

- Bodies established on the territory of the European Union, whether or not the processing takes place in the EU;
- Organisations located outside the EU, whose activity targets persons who are on the territory of the EU.

For more information:
Art. 2 and Art. 3 GDPR

2. Personal data

"Personal data" means any information relating to an identified or identifiable natural person ("data subject").

An 'identifiable natural person' is defined as a natural person 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, a political opinion or one or more specific elements of his or her physical, physiological, genetic, psychological, economic, cultural or social identity.

For more information :

Art. 4.1 GDPR

3. Data processing

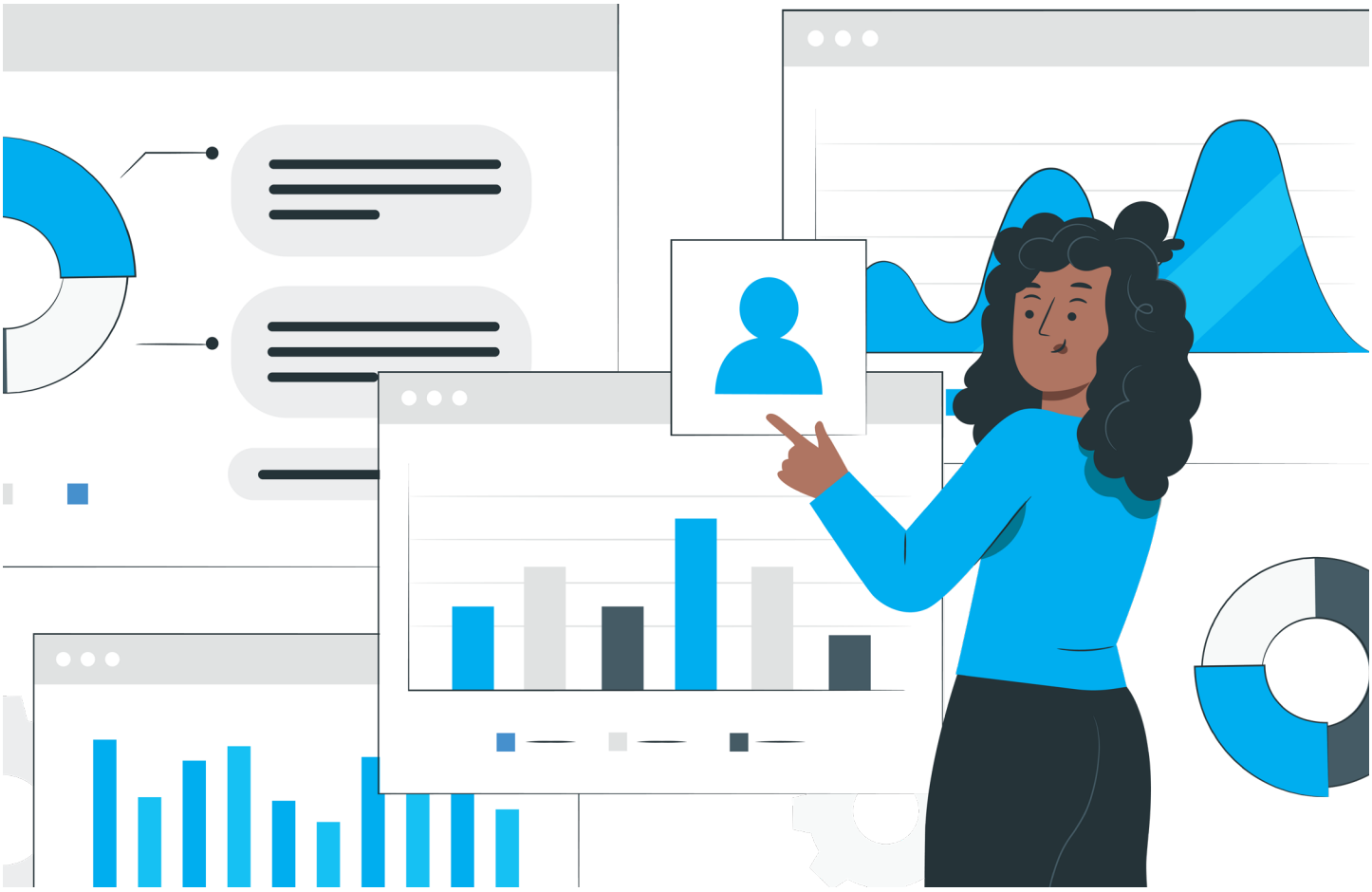
"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,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

For more information :

Art. 4.2 GDPR

SOME EXAMPLES OF DATA PROCESSING :

- HR data processing
- Salaries of wages
- Commercial prospecting
- Processing operation of customer data
- Suppliers and after-sales services



4. The Data Protection Officer

The main tasks of the Data Protection Officer (DPO) are:

- Inform and advise the organisation on the implementation of the GDPR;
- Monitoring compliance with the GDPR;
- Be a point of contact between the organisation, the CNPD and the data subjects.

For more information :

Article 39 GDPR and dedicated page on the notion of DPO of the CNPD website

Do you need a DPO?

The designation of a DPO is mandatory if:

- You are a public body;
- You are a company whose core business requires you to carry out regular and systematic monitoring of individuals on a large scale, or to process on a large scale so-called 'sensitive' data or data relating to criminal convictions and offences.
- In all other cases, designation is optional.

In which case should I appoint a DPO?

Some illustrations:

YES, You process personal data to serve targeted advertisements on search engines based on the on-line behaviour of data subjects.

YES, You are a bank that must regularly and systematically monitor the progress of its customers' accounts and transactions, particularly in the case of its obligations relating to the prevention of fraud, money laundering or terrorist financing.

No, You send an advertisement to your customers once a year to promote your local food business.

No,You are a general practitioner and you collect data about the health of your patients.

Yes, You process personal data relating to genetics and health on behalf of a hospital.

ENSURE COMPLIANCE WITH THE DATA PROTECTION PRINCIPLES

When processing personal data, you must comply with the following principles:

1. Collect personal data lawfully, fairly and transparently

The collection, storage, use and transmission of personal data must be in accordance with the GDPR, in good faith and not without the knowledge of the data subject.

2. Do not collect and process personal data without a specific purpose

Personal data must be collected for specified, explicit and legitimate purposes and may not be processed in a manner incompatible with those purposes (e.g. further use for another purpose).

3. Apply the principle of data minimisation

It is essential to process only the data that are necessary for the achievement of the purposes.

4. Ensure data is accurate and kept up to date

You must take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

5. Determine a proportionate storage period

The data must not be kept longer than necessary for the purposes for which they are collected and processed. Beyond that, the data must be deleted or anonymized.

6. Ensure data integrity and confidentiality

Sufficient data security must be ensured by appropriate technical and organisational measures, in particular against unauthorised or unlawful processing and against accidental loss, destruction or alteration of data.

7. 7. Demonstrate your compliance ("accountability")

You must take appropriate measures to ensure and be able to demonstrate that the processing of personal data is carried out in compliance with the GDPR.

What is the conflict of interest?

The DPO may carry out other tasks and tasks, provided that they do not give rise to a conflict of interest. The DPO cannot perform a function within the organisation that would lead it to determine the means (how?) and purposes (why?) of data processing. This should be considered on a case-by-case basis.

IDENTIFY THE BASIS OF LAWFULNESS FOR YOUR DATA PROCESSING

To be lawful, data processing must be based on one of the following six conditions:

1. The consent of the data subject (separate for each purpose);
2. The performance of a contract;
3. A legal obligation (clear and precise);
4. The vital interest of the data subject or another person;
5. The performance of a task carried out in the public interest, or
6. The legitimate interest of the controller (e.g. for marketing, anti-fraud purposes, processing of customer or employee data, security of processing, etc.).

Consent must be "free, specific, informed and unambiguous", i.e. the data subject must have a genuine choice.

If you collect data related to children via your commercial website (e.g. online games, social networks), it is necessary to obtain parental consent.

Information about users must be easy to understand and formulated in simple and clear terms.

For more information:

Articles 5 to 9 GDPR and see Fact Sheet No. 3 on the criteria for consent

IDENTIFY DATA PROCESSING ACTIVITIES NEEDING SPECIAL VIGILANCE

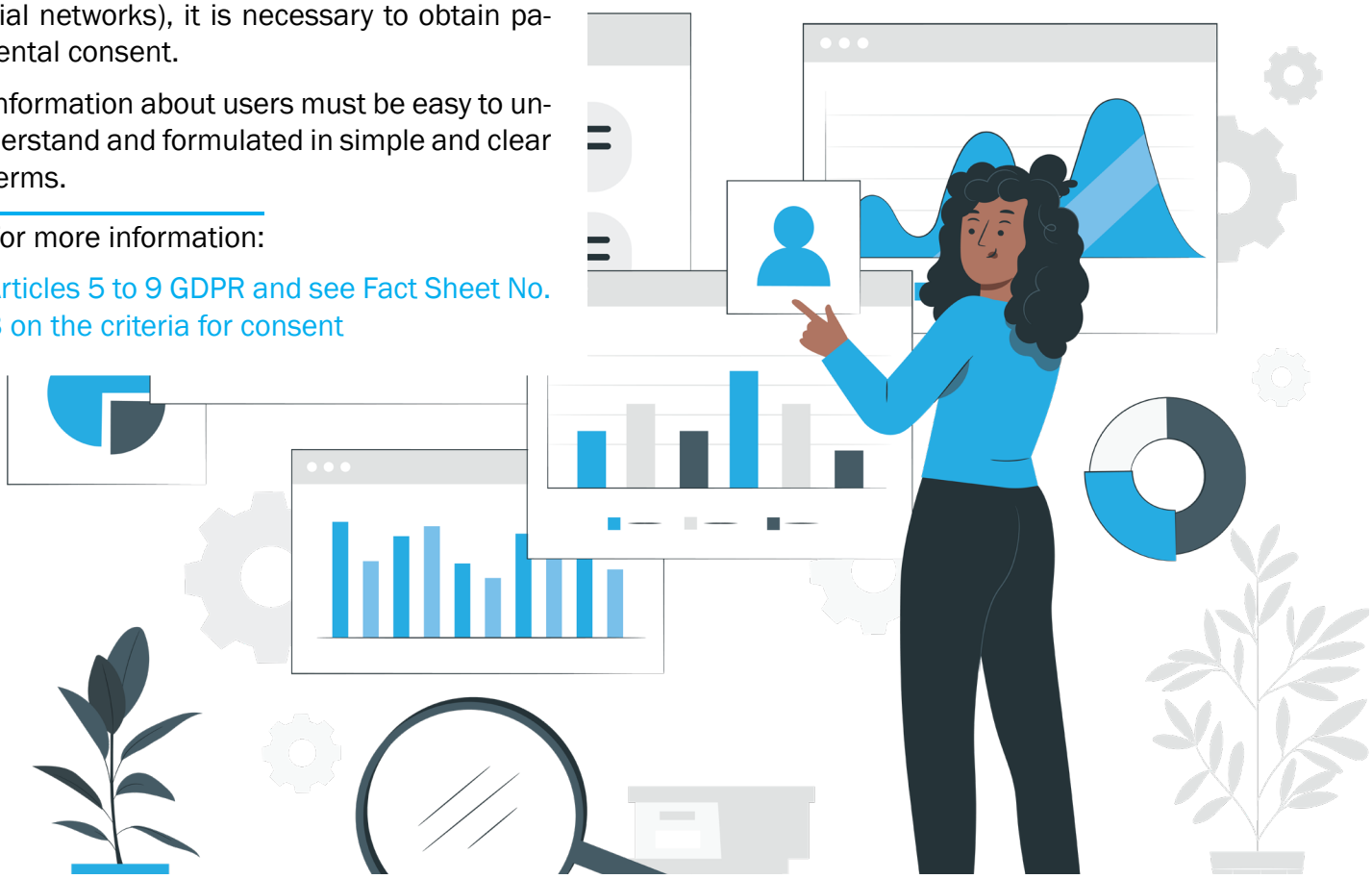
You process certain types of "sensitive" data

- Data revealing alleged racial or ethnic origin, political, philosophical or religious opinions, trade union membership;
- Data concerning health or sexual orientation;
- Genetic or biometric data;
- Criminal offence or conviction data;
- Data concerning minors.

Your processing has the object or effect

- Systematic large-scale monitoring of a publicly accessible area;
- Systematic and thorough assessment of personal aspects, including profiling, on the basis of which you make decisions that produce legal effects on or significantly affect a natural person.

If your treatments meet any of the characteristics listed above, special measures or rules may apply (examples: data protection impact assessment, enhanced information, collection of consent, contractual clauses, etc.).



RESPECT INDIVIDUAL RIGHTS

The main objective of the GDPR is to strengthen individuals' control over their data. To this end, the Regulation provides for various rights:

1. The right to be informed

You must inform data subjects that their personal data is being processed, by whom and why. This information must be presented in plain and clear language at the time the data are collected, or if the data have not been collected from the person himself, generally within a reasonable period of time not exceeding one month.

2. The right of access

If a person asks you whether you hold information about them, you must confirm that personal data relating to them are or are not being processed and, where applicable, provide them with a copy of all the data you hold about them.

3. The right to rectification

You have an obligation to ensure that the data you collect is accurate and, if necessary, kept up to date. At the request of a data subject, you must rectify inaccurate information.

4. The right to be forgotten

Where a person no longer wishes the data relating to him or her to be processed, you have an obligation to delete that data unless there is a legitimate reason for keeping it.

For example, a citizen may require the immediate removal of personal data collected or published on a social network when he or she was still a child and was not fully aware of the risks inherent in the processing.

5. The right to data portability

When a data subject wishes to retrieve the data that he or she has provided to you, you must be able to return them in a structured, commonly used and machine-readable format in order to allow him or her to transmit them to another body (social network, internet service provider, streaming site, etc.).

6. The right to object

Where a data subject exercises the right to object at any time, on grounds relating to his or her particular situa-tion, to processing of personal data which is necessary for the pursuit of your legitimate interests or for the performance of a task carried out in the public inter-est, you must stop the processingunless you can demonstrate compelling legitimate grounds for the continuation of the processing. You must also respect the data subject's right to object, without justi-fication, to the use of his or her data for ideologically oriented commercial prospecting or canvassing pur-poses (political parties, trade unions, religious groups, etc.).

7. The right to limitation

As a controller, you must suspend the processing of personal data where a data subject claims the restriction of the processing of his or her data, i.e.:

- They dispute the accuracy of one of the data. The suspension will last for as long as you need to verify its accuracy;
- The processing is unlawful and they nevertheless opposes its erasure, preferring such a limitation;
- Since it is no longer necessary, the data subject needs it for the establishment, exercise or defence of his or her rights in court.

The limitation may be carried out in various ways (temporary movement to another file, blocking of data, temporary removal from a website, etc.).

For more information :

Articles 13 to 22 GDPR and the dedicated page of the CNPD website

FOCUS:

MANAGEMENT OF THE RIGHT OF ACCESS

1. Content of the reply to a request for a right of access

Where a data subject exercises their right of access, the controller must provide them with a copy of the data concerning them and the following information:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients established in third countries or international organisations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Finally, where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

2. Response time

A reply to a request for access must be communicated as soon as possible and in any event no later than one month after receipt of the request.

If necessary, this period may be extended by two months, taking into account the complexity and number of applications. In this case, the controller must inform the data subject of this extension and the reasons for the postponement within one month of receipt of the request.

This period is the same for all individual rights.

3. Verification of identity, in case of doubt

When faced with a request from a person to exercise their rights, verification of their identity is essential.

The level of verification required may vary depending on the nature of the request, the importance of the information provided and the specific context of the request.

As a matter of principle, it is necessary to avoid requesting a copy of the person's identity card, as this identity verification can be carried out 'by any means'.

For example, the data subject may provide you with additional information such as a customer or membership number, in order to confirm his or her identity. The person can also prove his/her identity by exercising his/her rights from a space where he/she has previously authenticated himself/herself.

However, in case of "reasonable doubt" about a person's identity, you can ask them to provide other documents to confirm their identity, including a copy of the identity card.

4. A non-absolute right, in principle free of charge

The exercise of the right of access is in principle free of charge.

The body must facilitate the exercise of the rights of the individuals concerned by the processing of the data. He cannot refuse to comply with a request without justifying it to the person.

The organisation may not comply with a request if:

- Its implementation infringes the rights or freedoms of others (in particular with regard to trade secrets, intellectual property and copyright protecting software);
- A person's requests are manifestly unfounded or excessive, in particular because they are repetitive: in this case, the controller may alternatively choose to respond by requiring the payment of a reasonable fee that takes into account the administrative costs incurred in providing the information, making the communications or taking the action requested;

If the body chooses not to comply with the request, it must then inform the data subject within one month, stating the reasons for its choice and informing him or her of the possibility of lodging a complaint with the CNPD and/or seeking a judicial remedy.