Level 3

Implementation: data breach, transfers and data processing agreement

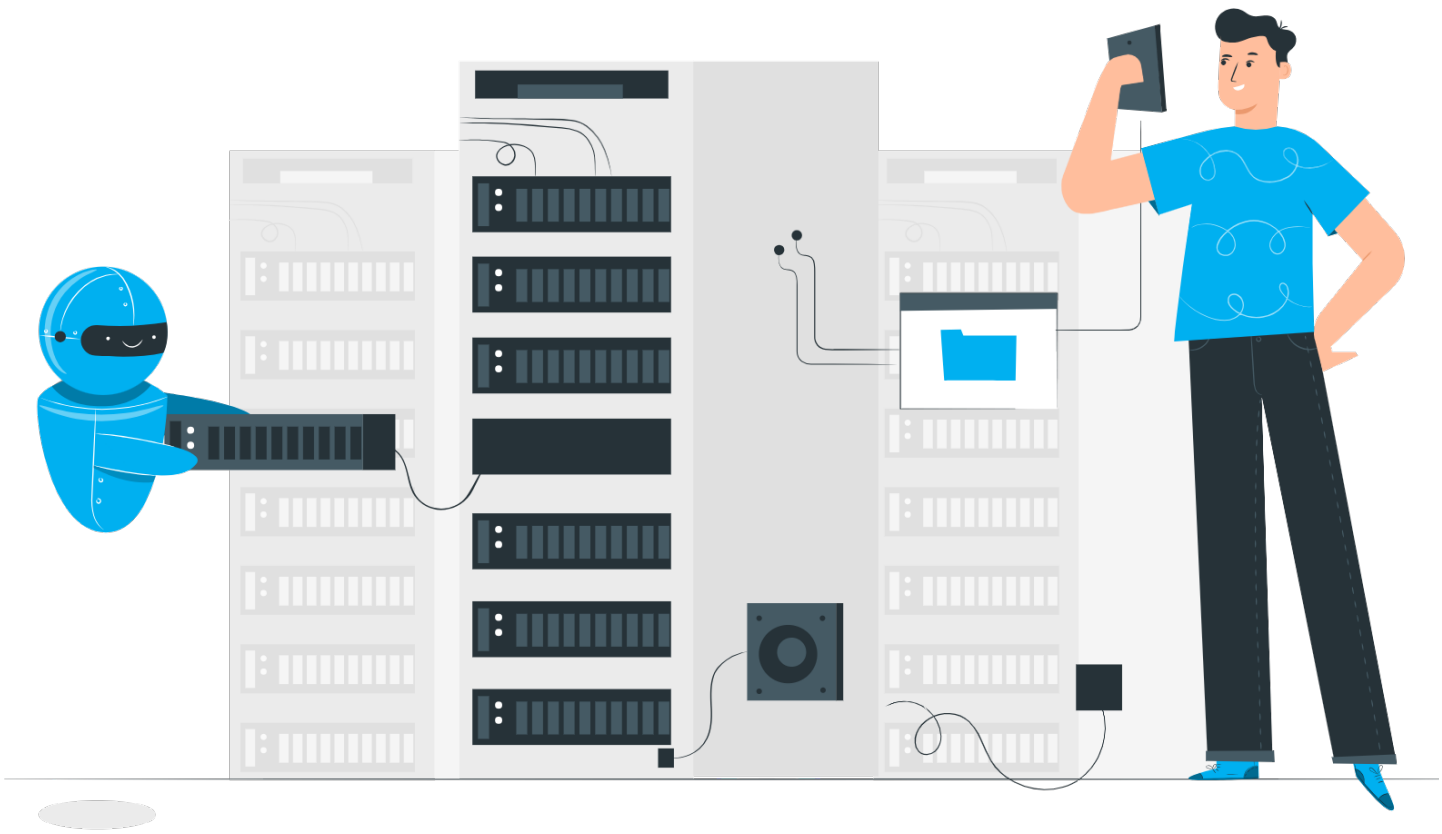
Key words: Anonymisation, data breach, data breaches register, encryption, confidentiality, data processing agreement, information of data subjects, liability, notification, personal data of employees, pseudonymisation, rights and freedoms of data subjects, risks, standard contractual clauses, technical and organisational security measures, third countries, transfers

Luxembourg House of Cybersecurity

CNPD National Commission for Data Protection Grand-Duchy of Luxembourg

Co-funded by the European Union

Update : 4th June 2024



Good to know

Luxembourg House of Cybersecurity (LHC)

LHC is the backbone of state-of-the-art cyber resilience in Luxembourg and aims to capitalise on and further develop innovation, skills, collaboration and capacity building.

As a central player, the LHC is home to all types of cyber security activities. With its two centres, CIRCL (Computer Incident Response Center Luxembourg) and NC3 (National Cybersecurity Competence Center) and with key partners, LHC supports, nurtures and serves a wide range of sectors, such as the private, public, health, education and industrial sectors.

Computer Incident Response Center Luxembourg

CIRCL is a government initiative designed to collect, review, report and respond to computer security threats and incidents.

CIRCL provides a reliable and trusted point of contact for all users, companies and organisations based in Luxembourg, for the handling of attacks and incidents. The objective of CIRCL is to collect, investigate, report and respond to cyber threats in a systematic and timely manner.

KNOW HOW TO REACT IN CASE OF A DATA BREACH!

1. Data breach concepts

What is a data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data breaches can be categorized according to the three well-known principles of information security:

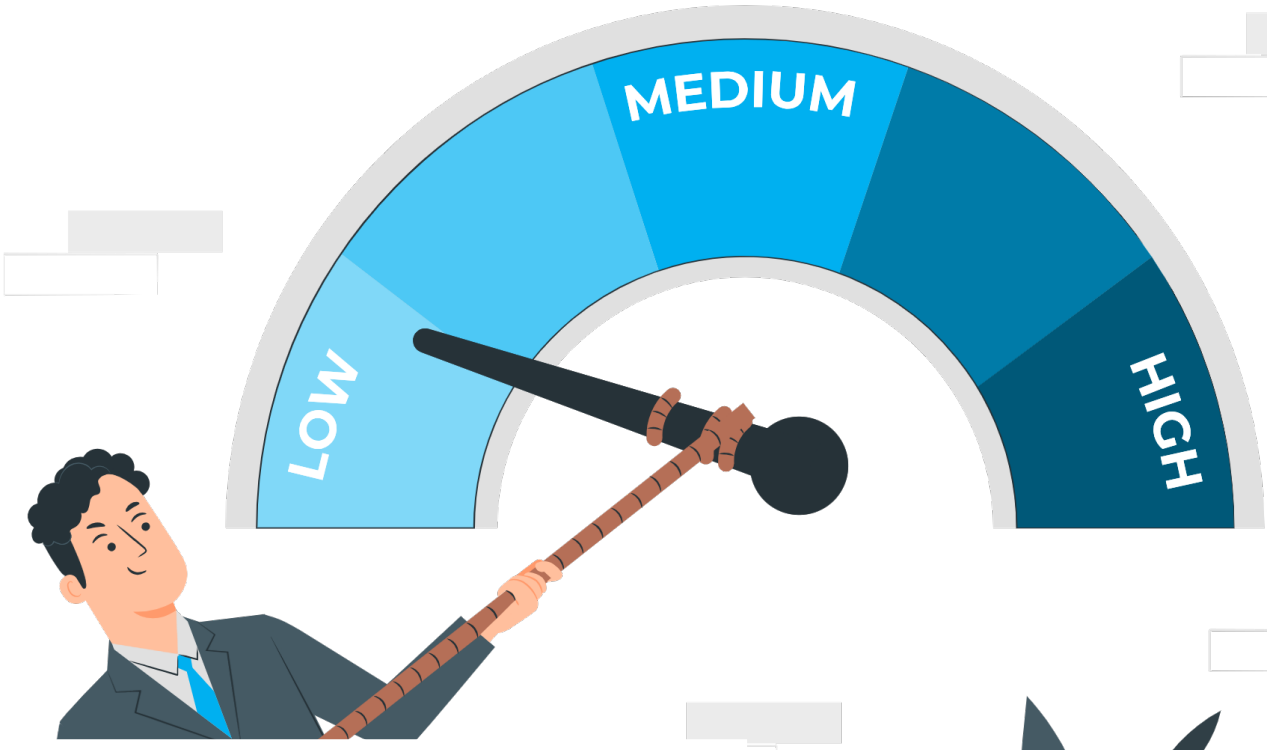
- **Breach of confidentiality:** en cas de divulgation ou d'accès non autorisé ou accidentel à des données à caractère personnel
- **Breach of availability** in case of loss /accidental or unauthorized destruction of personal data
- **Integrity breach :** in case of accidental or unauthorized modification of personal data

Depending on the circumstances, a breach may concern the confidentiality, the integrity and the availability at the same time, as well as any combination of these three principles.

Recital 85 GDPR: A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

What to do in the event of a data breach?

The controller shall identify whether the data breach presents a risk to the rights and freedoms of the data subjects. Controllers may use their replies to notification form as a basis for determining whether the breach poses a risk to data subjects.



When and how to notify the CNPD ?

If the data breach results in a risk to the rights and freedoms of individuals, a notification of the breach to the CNPD is required within 72 hours of becoming aware of it.

The notification form can be used to make the notification.

The notification must, at least:

1. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. Describe the likely consequences of the personal data breach;
4. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The notification of the violation shall be sent to the email address databreach@cnpd.lu. You may use the downloadable gpg public key to secure the transmission of information by encrypting it

Good to know:

The risk is defined, among other things, by the degree of sensitivity of the data processed as well as the severity and likelihood of impact on the fundamental rights and freedoms of the data subjects (body, material, moral impacts, etc.). For example, managing the members of a non-profit association requires a lower degree of security than the management of a medical file by a doctor.

Good to know:

The reference to the fundamental rights and freedoms of natural persons mainly refers to data protection and the protection of privacy but also extends, where appropriate, to other fundamental rights, such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty and freedom of conscience and religion.

When and how to notify data subjects about the data breach ?

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least:

1. The name and contact details of the data protection officer or other contact point where more information can be obtained;
2. A description of the likely consequences of the personal data breach;
3. A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The means of communication used to contact the data subjects must be effective. There must be a high probability that they receive the necessary information. If necessary, public communication may be required.

Keep a data breach register

Whether the risk is high or non-existent, the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

The National Commission may request access to this documentation to verify compliance by the controller or processor with the GDPR.

What will the CNPD do following receipt of the notification?

As soon as the notification is received, the National Commission will:

- Send an electronic acknowledgement of receipt (to the same address that sent it);
- Check the notification and, if necessary, contact the controller to verify the authenticity of the notification;
- Depending on the circumstances, contact the controller in case of questions – including the need to inform the data subjects or not.

The processing of the notification by the National Commission will focus strongly on the management of the incident by the controller and, where appropriate, on the communication to the data subjects.

Responsibilities of processors

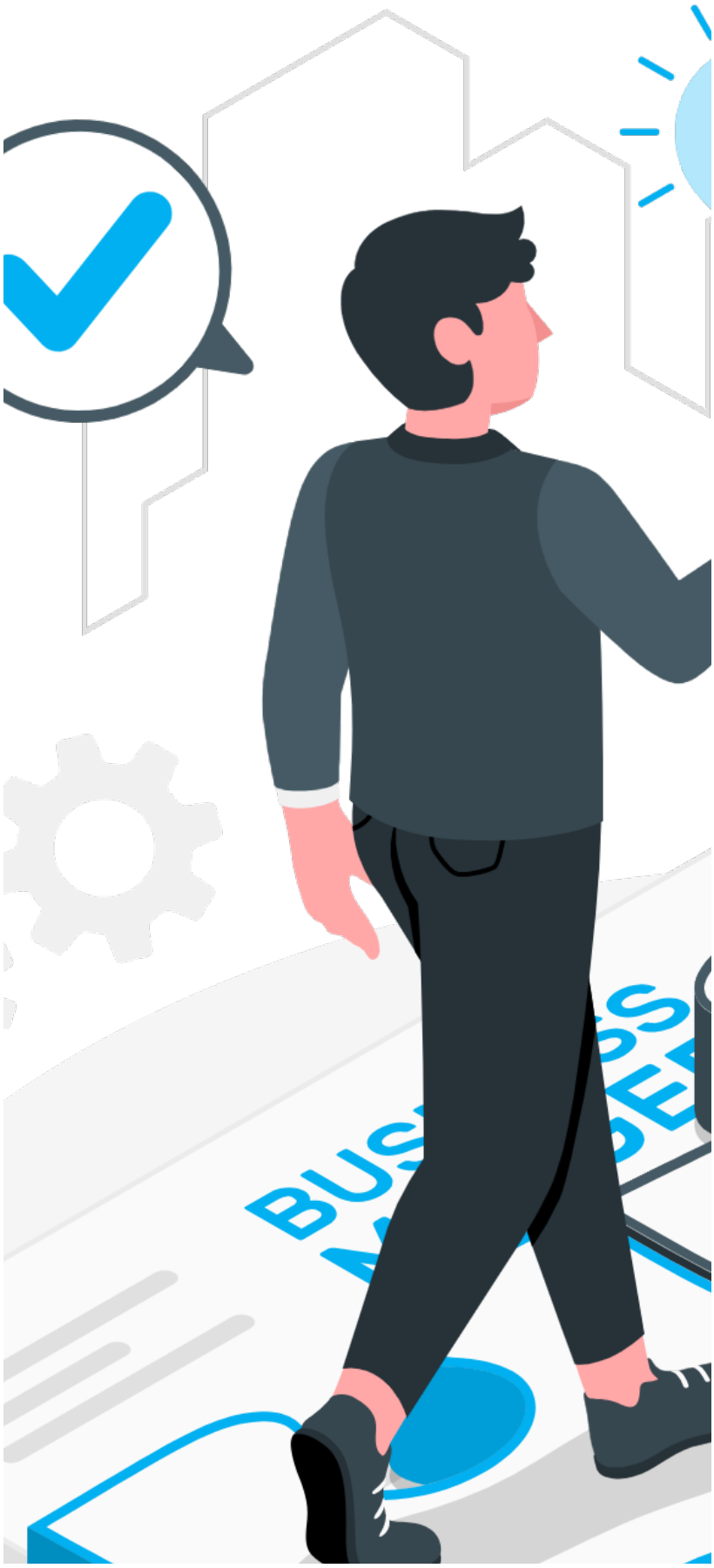
Data processors are responsible for setting up organizational and technical measures to be able to notify the controller without undue delay after becoming aware of a personal data breach in order for the latter to be able to comply with the 72 hours notification period after the incident is detected.

What to do after the data breach?

Il est important pour une entité d'adapter les mesures de sécurité organisationnelles et techniques à ses traitements pour éviter que le même type de violation puisse se reproduire.

Confidentiality of the breach

It is not the within the competence of the National Commission to make a data breach public. However, a controller may, by his own decision or at the request of the National Commission, communicate about a data breach in public if it is likely to result in a risk to the rights and freedoms of natural persons and if they cannot be contacted effectively by any other means.



2. 2. TECHNICAL AND ORGANISATIONAL MEASURES

Ensuring a level of security appropriate to the risk

One of the requirements of the GDPR is that personal data be processed in such a way as to ensure an appropriate level of security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR therefore requires controllers and processors to put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the personal data processed. They should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks to the rights and freedoms of natural persons posed by the processing, the likelihood and severity of which vary. The GDPR also requires that all appropriate technical and organisational protection measures are implemented to immediately establish whether a personal data breach has occurred, which will determine whether the notification obligation applies.

Following an incident, it is important for an entity to adapt organisational and technical security measures to its processing operations to prevent the same type of breach from reoccurring.

Illustrations of security measures

- **Encryption**

Data encryption translates data into another form, or code, so that only people with access to a secret key (called a decryption key) or password can read it. Encrypted data is commonly referred to as encrypted text, while unencrypted data is referred to as plain text. Currently, encryption is one of the most popular and effective data security methods used by companies.

The current state of knowledge is to be taken into account, an outdated technology will not be considered valid.

- **Pseudonymisation**

Pseudonymisation consists of replacing the directly identifying data (surname, first names, etc.) of a dataset with indirectly identifying data (aliases, sequential number, etc.). Pseudonymisation thus makes it possible to process the data of individuals without being able to identify them directly. Unlike anonymisation, pseudonymisation is a reversible operation: the identity of a person can be traced if additional information is available.

- **Anonymisation**

Anonymisation is the processing of personal data which consists in using a set of techniques in such a way as to make it impossible, in practice, to re-identify the person by any means. This operation is irreversible, so that it is no longer possible to trace a person's identity.

Anonymisation opens up potential for the re-use of data and thus allows actors to exploit and share their data pool without infringing on the privacy of individuals. It also makes it possible to keep data without limitation.

It should be noted that in practice anonymisation is a destructive information technique. It is therefore advisable to use anonymisation when:

- has sufficient amounts of data
- has a clear idea of how the anonymised data will be used
- is able to implement an anonymisation method that will retain the desired properties of the dataset.

To build a relevant anonymisation process, it is advisable to:

- examine the categories of data to be anonymised (structured or unstructured data, time series, geolocation information, etc.)
- remove direct identifiers as well as rare values that could allow easy re-identification of individuals (e.g. precise knowledge of the age of individuals present in a dataset can make it very easy in some cases to re-identify centenarians)
- distinguish important information from secondary or unnecessary information (i.e. deletable, which is best not collected at all under the data minimisation principle)
- define the ideal and acceptable fineness for each piece of information retained
- defining priorities (example: Is it more important to keep a high level of finesse on this information or to keep this other information?).

CONTROL OF DATA TRANSFERS TO THIRD COUNTRIES!

What is a third country?

A third country is a country which is not bound by the General Data Protection Regulation (GDPR) - as opposed to the 28 Member States of the EU and the three European Economic Area (EEA) countries Norway, Liechtenstein and Iceland.

Transfer within the European Economic Area

Personal data may move freely from the Grand Duchy of Luxembourg within the European Economic Area (European Union, Liechtenstein, Norway and Iceland), as long as the general principles of the GDPR are respected.

Indeed, Member States apply the same level of protection when processing personal data. A transfer within the European Economic Area is therefore governed in the same way as a transfer to Luxembourg and must therefore comply with the general principles of the GDPR (compliance, in particular, with the principle of lawfulness, compatibility of the communication with the original processing, information of data subjects).

Transfer to a third country recognised as providing an adequate protection

Third countries can be recognised, on the basis of an adequacy decision of the European Commission, as ensuring a suitable level of protection of personal data to enable the transfer of personal data from EU and EEA Member States to these countries.

To date, the European Commission has recognised that Andorra, Argentina, Canada (only trade organisations), South Korea, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the United Kingdom, Switzerland, Uruguay and the United States (only for trade organisations participating in the EU-US Data Privacy Framework) provide an adequate protection (on 1 January 2024).

The consequence of this decision is that personal data may be transferred from the EU and EEA Member States to the secure third country (within the material scope described by each decision) without additional requirements.

TRANSFER TO A THIRD COUNTRY NOT RECOGNISED AS PROVIDING AN ADEQUATE PROTECTION

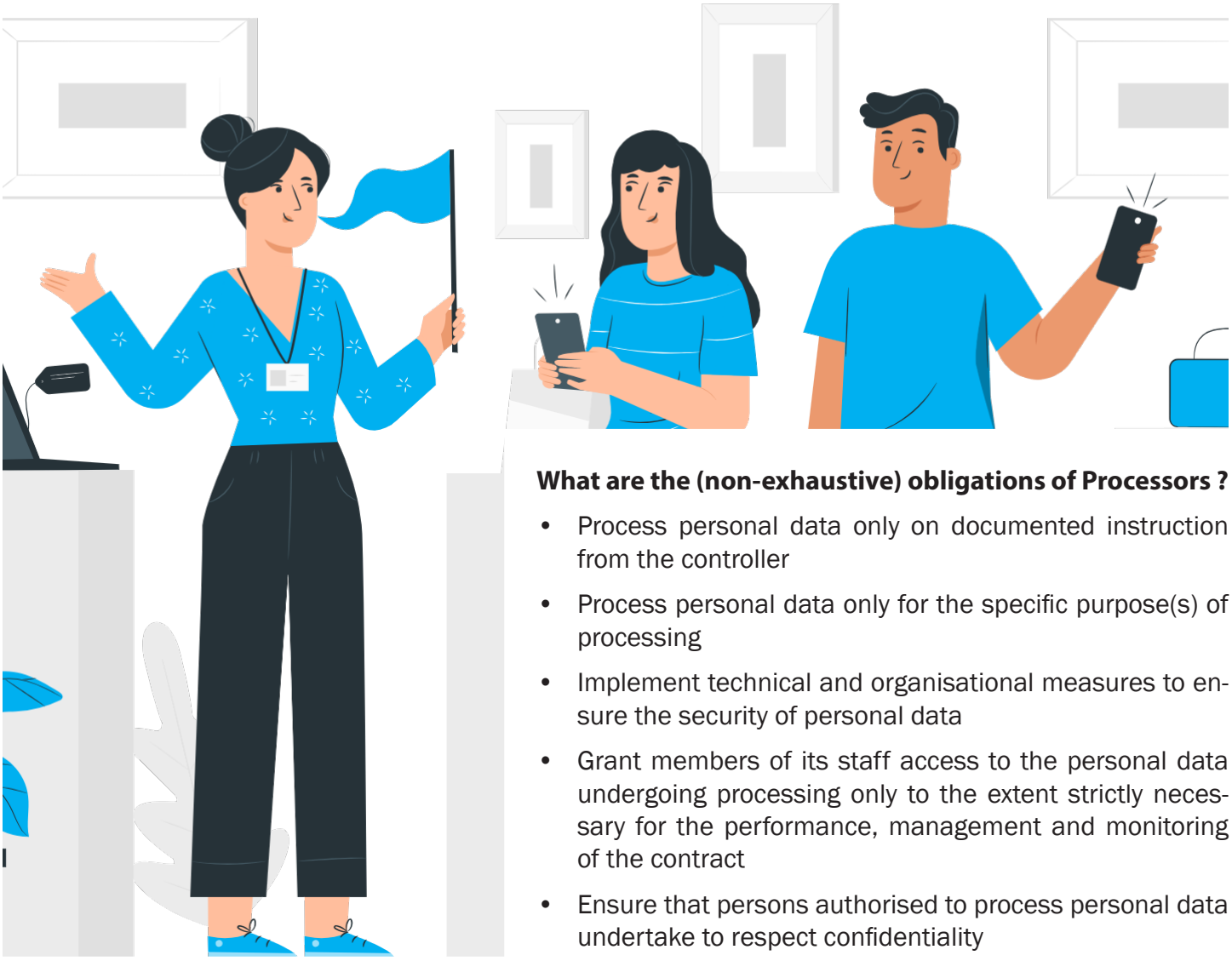
There are various safeguards available to controllers or processors who wish to transfer personal data to a country outside the European Economic Area that does not have an adequate level of protection.

These controllers and processors can rely in particular on the standard contractual clauses (SCCs) adopted by the European Commission, which are a model contracts for the transfer of personal data. These SCCs were updated on 4 June 2021 and replace the previously applicable SCCs. They are distinct from the SCCs for data processing relationships. These are the most appropriate safeguards for small and medium-sized enterprises.

Binding corporate rules (BCRs) ensure an adequate level of protection for data exchanged within a group of companies located both inside and outside the European Economic Area. BCRs are ideal for a multinational group of companies that carries out a large number of international data transfers.

Since the entry into force of the GDPR on 25 May 2018, new transfer mechanisms are available to controllers or processors, who intend to transfer personal data to a third country with no adequate level of protection. These are:

- - approved codes of conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and
- - approved certification mechanisms pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.



GIVE INTEREST TO THE DATA PROCESSING AGREEMENT (Article 28 GDPR)!

Why manage data processing?

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play in enabling the controller to comply with its obligations and this includes notification of a breach.

What are the (non-exhaustive) obligations of Processors ?

- Process personal data only on documented instruction from the controller
- Process personal data only for the specific purpose(s) of processing
- Implement technical and organisational measures to ensure the security of personal data
- Grant members of its staff access to the personal data undergoing processing only to the extent strictly necessary for the performance, management and monitoring of the contract
- Ensure that persons authorised to process personal data undertake to respect confidentiality
- Apply specific limitations and/or additional safeguards in case of processing of sensitive data
- Prompt and adequate processing of requests from the controller concerning the processing of data
- Allow audits of processing activities to be carried out at the request of the controller
- Use the services of a sub-processor to carry out specific processing activities, only with the prior, specific or general written authorisation of the controller. Irrespective of the specific or general nature of this prior authorisation, the initial processor must keep an up-to-date list of other sub-processors.