EN

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Your data protection obligations

Guide for businesses, public authorities and associations

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette

cnpd.public.lu

As of 25 May 2018, the General Data Protection Regulation will impose stricter accountability obligations on private and public actors, as well as their sub-contractors. They will be required to constantly ensure that the rules set out in the Regulation are followed and must be able to document their compliance with these rules at all times.

In Luxembourg, the National Commission for Data Protection (in French: Commission nationale pour la protection des données - CNPD) supervises the lawfulness of processing activities, covering the collection, use and transfers of data relating to identifiable individuals. It also protects the freedoms and fundamental rights of natural persons, in particular their right to privacy.

[!] PERSONAL DATA CAN BE THE FOLLOWING:

- name,
- address,
- national identification number,
- health related data,
- e-mail address,
- telephone number,
- political opinion,
- etc.

[?] YOU COLLECT, USE OR PROCESS PERSONAL DATA?

Yes? The Regulation applies and you must respect the rules!

[?] YOU PROCESS PERSONAL DATA ON BEHALF OF ANOTHER ORGANISATION?

The Regulation applies to you as well.

[?] ARE YOU A CONTROLLER OR A PROCESSOR?

Controller:
determines the purposes and means of the processing of personal data

Processor:
processes personal data on behalf of the controller

Your obligations

Start preparing the inventory of all your processing operations (e.g. employee data, client data, etc.). Consider in particular the following questions: what is the current legal basis and the purpose of the data processing? Where and how are the data collected and who are the recipients? Where are the data stored and who has access to them?

[!] Apply the main data protection principles

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

PROCESS PERSONAL DATA IN A LAWFUL, FAIR AND TRANSPARENT MANNER

Personal data may only be collected, recorded, used and transferred in compliance with the Regulation, in good faith and transparently for the data subject.

ONLY COLLECT PERSONAL DATA WITH A CLEARLY DEFINED PURPOSE

Personal data must be collected for specified, explicit and legitimate purposes and cannot be further processed in a manner that is incompatible with these purposes (e.g. further use for other purposes).

APPLY THE PRINCIPLE OF DATA MINIMISATION

You must only process the data that are necessary to achieve the chosen purposes.

ENSURE THAT THE DATA ARE ACCURATE AND KEPT UP TO DATE

You must take all reasonable steps to ensure that incorrect data are rectified or deleted without delay.

SET A PROPORTIONATE STORAGE DURATION

You must not retain data for longer than is necessary for the achievement of the purposes for which they were collected and processed. At the end of the retention period, the data must be deleted or anonymised.

ENSURE THE INTEGRITY AND THE CONFIDENTIALITY OF THE PERSONAL DATA

You must guarantee an appropriate level of security to protect the data, in particular against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate organisational and technical measures.

DEMONSTRATE YOUR COMPLIANCE ("ACCOUNTABILITY")

You have to put measures in place to comply with the Regulation and be able to demonstrate compliance.

[!] Identify the legal basis for your processing

In order to be lawful, the processing operations must be based on one of the following conditions:

1. the consent of the data subject (separate for each purpose);
2. a contract;
3. a legal obligation (which is clear and precise);
4. the vital interest of the data subject or of another person;
5. a task carried out in the public interest;
6. the legitimate interest of the controller (e.g. for the purposes of direct marketing or of fraud prevention, the processing of client or employee data, security measures undertaken by the controller).

Consent must be "free, specific, informed and unambiguous", which means that the data subject must have a genuine choice.

If you collect data relating to children via your website (e.g. online game, social networks), the consent of the parents is required. The information provided to the users must be easy to understand, using clear and plain language.

Identify the processing operations that require particular attention

YOU PROCESS SPECIAL CATEGORIES OF DATA

- data which reveal the racial or ethnic origin, political opinions; philosophical or religious beliefs, trade union membership;
- data concerning the health or sexual orientation of the data subject;
- genetic or biometric data;
- data relating to criminal convictions and offences;
- data relating to minors.

WITH THE PROCESSING, YOU

- systematically monitor a publicly accessible area on a large scale;
- systematically and extensively evaluate the personal aspects of natural persons on the basis of automated processing, and on which decisions are based that produce legal effects concerning that natural person or similarly significantly affect that natural person.

Where your processing operation involves one of the above scenarios, specific conditions may apply (e.g. a data protection impact assessment, additional information to be provided to the data subject, the consent of the data subject, contractual clauses, etc.).

Protect the data from the beginning

Implement appropriate security measures at the earliest stages of the software or product development ("Data protection by design").

Adopt measures to ensure that, by default, only personal data, which are necessary for each specific purpose, are processed ("Data protection by default"), e.g. the automatic deletion of personal data which are no longer necessary.

Ensure that your processors are aware of their obligations

Only choose processors that provide sufficient guarantees to ensure the protection of the personal data processed. Conclude a contract that sets out the processor's obligations concerning the security, the confidentiality and the protection of the processed personal data.

Ensure that appropriate security measures are implemented

Both you and your processors must implement appropriate security measures, taking in account the risks to the data subjects and the type of personal data processed.

Notify data breaches to the CNPD

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, you must inform the CNPD of the breach. In certain cases, you must also inform the data subjects of the breach.

Determine whether you transfer data outside the European Union

If the European Commission does not recognise the country to which you are transferring personal data as adequate, you must provide appropriate safeguards when transferring personal data outside the European Union.

Comply with the rights of data subjects

1/ Information to the data subject

You must inform data subjects that their personal data are processed, as well as who processes the data and why they are being processed. The information must be provided using clear and plain language and must be given at the time when the data are collected. Where the data are not collected directly from the data subject, the information must generally be provided within a reasonable period of time, but no later than a month after the collection.

2/ The right to contest a decision based solely on automated processing

If you adopt a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject (e.g. the approval for a loan or an insurance contract), you must grant the data subject the right to express his or her point of view and to contest the decision. You must also inform the data subject of the logic involved in the decision-making.

3/ The right of access

If a data subject asks whether you hold information on him or her, you must state whether you do and, if requested, you must give the person a complete copy of the personal data relating to him or her.

4/ The right to rectification

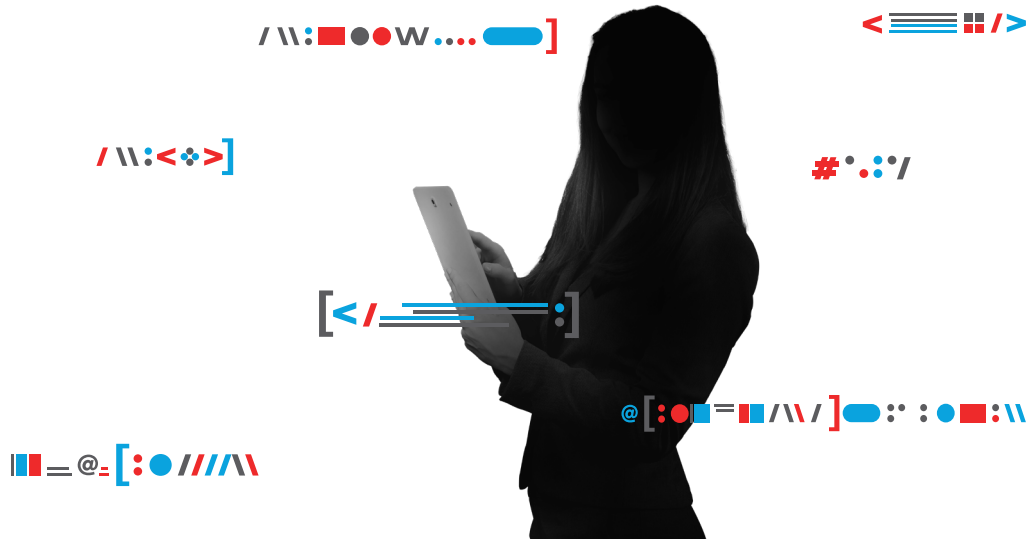
You must only collect and process data that are accurate and up to date. At the request of a data subject, you must rectify any incorrect data.

5/ The right to be forgotten

Where a person no longer wishes for their personal data to be processed, you must delete the data, unless you have a legitimate reason to keep them. For example, a data subject may request the immediate removal of personal data, which were collected or published on a social network, while the data subject was a child.

6/ The right to data portability

A data subject must be able to receive the personal data, which have been provided to an organisation, in a structured, commonly used and machine-readable format and to transmit those data to another organisation (social network, Internet access provider, streaming website, etc.).



7/ The right to object

The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of his or her personal data, which is necessary for the purposes of the legitimate interests of your organisation or which is necessary for the performance of a task carried out in the public interest. In such a case, you can no longer process the personal data, unless there are compelling legitimate grounds to continue the processing activity.

You must also respect the right of the data subject to object to the use of his or her personal data for direct marketing purposes or canvassing purposes (political parties, unions, religious organisations, etc.), without requiring the data subject to justify the objection.

8/ The right to restriction of processing

The data subject can request the restriction of processing:

- if the person contests the accuracy of the personal data, for the time required to check the accuracy;
- if the processing is unlawful and the person objects to the erasure of the data;
- if you no longer need the personal data, but the data subjects needs it for the establishment, exercise or defence of legal claims.

Where the processing has been restricted, the data can no longer be processed. The method used to restrict the process may vary depending on the situation (temporary move to another file, locking of data, temporary removal from a website, etc.).

Do you need a data protection officer?

The appointment of a data protection officer is obligatory, if:

- you are a public authority or body;
- you are a company whose core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale, or which consist of large scale processing of "sensitive data" and data relating to criminal convictions and offences.

In all other cases, the appointment of a data protection officer is optional.

?

When do I have to appoint a data protection officer?

YES You process personal data to display **targeted advertising on search engines** based on the online activities of the data subjects.

YES You are **a bank which must regularly and systematically monitor the accounts and transactions of its clients**, in particular as a part of your anti-money laundering and fraud prevention obligations.

NO You send an advertisement to your clients once a year to promote your local grocery shop.

NO You are a general practitioner and you collect the health related data of your patients.

YES You process **genetic and health** related data on behalf of a hospital.

Manage the risks

If you have determined that the processing is likely to result in a high risk to the rights and freedoms of data subjects, you must carry out a **data protection impact assessment** (DPIA) for each processing operation.

A data protection impact assessment is required if several of the following criteria apply:

- The processing operation involves an evaluation or scoring, including profiling and prediction.
- The processing operation involves automated decision-making with legal effects for the data subjects or similarly significantly affects them.
- The processing involves systematic monitoring (the processing is used to observe, monitor or control data subjects, including data collected through a systematic monitoring of a publicly accessible area).
- The processing operation includes sensitive data (according to the definition of the Regulation).
- Data are processed on a large scale. To determine whether the processing activity is large scale, account should be taken of:
  - the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
  - the volume of data and/or the range of different data items being processed;
  - the duration, or permanence, of the data processing activity;
  - the geographical extent of the processing activity.
- Datasets have been matched or combined in a way that could exceed the reasonable expectations of the data subject.
- The data processed relate to vulnerable data subjects (e.g. there is a power imbalance between the data subjects and the data controller).
- The processing operations involve the innovative use or application of technological or organisational solutions.
- The processing in itself prevents data subjects from exercising a right or using a service or a contract (e.g. where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan).

When do I have to carry out a DPIA?

YES

A hospital processing its patients' genetic and health data (hospital information system).

Possible relevant criteria:

- sensitive data;
- data concerning vulnerable data subjects;
- large scale processing;

YES

The use of a **camera system to monitor** driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.

Possible Relevant criteria:

- systematic monitoring;
- innovative use or applying technological or organisational solutions.

YES

A company **monitoring its employees** activities, including the monitoring of the employees' work station, internet activity, etc.

Possible Relevant criteria:

- systematic monitoring;
- data concerning vulnerable data subjects.

NO

An online magazine using a mailing list **to send a generic daily** digest to its subscribers.

Possible Relevant criteria:

- none.

NO

An e-commerce website displaying adverts for vintage car parts involving **limited profiling based on past purchase(s)** behaviour on certain parts of its website.

Possible Relevant criteria:

- evaluation or scoring, but not systematic or extensive.

Document your processing activities

To demonstrate your compliance with the Regulation, you must maintain the necessary documentation. To continuously ensure the protection of the personal data you processed, you must regularly audit the actions and documentation relating to every phase of the processing operations.

You should in particular have the following records:

THE DOCUMENTATION RELATING TO YOUR PROCESSING ACTIVITIES

- the record of processing activities (for controllers) or categories of processing activities (for processors);
- the data protection impact assessments carried out for the processing activities which are likely to result in high risks for the rights and freedoms of data subjects;
- the framework for transfers of personal data outside the European Union (in particular standard data protection clauses, binding corporate rules and certification mechanisms);
- the record of all personal data breaches, which must set out the consequences of the breach as well as the remedial action taken.

INTERACTION WITH THE DATA SUBJECTS

- the information to the data subjects;
- the manner in which the consent of the data subject is obtained;
- the procedures in place to enable data subjects to exercise their rights.

THE DOCUMENTATION SPECIFYING THE ROLES AND RESPONSABILITIES OF THE ACTORS INVOLVED

- the contracts with processors;
- the internal procedures in the event of a data breach;
- the evidence that data subjects have given their consent, if consent is the lawful condition for processing.

Attention: This is not an exhaustive list and the required documentation may vary from one organisation to another.

Understand the sanctions

In the event of a violation of the Regulation, the CNPD has several corrective powers, amongst others, the power to order the erasure of the personal data or the temporary or definitive limitation on processing.

The CNPD will also have the power to impose an administrative fine of up to €20,000,000 or 4% of the total worldwide annual turnover.

Attention, In the event of an infringement of the Regulation, data subjects have:

- the right to an effective judicial remedy, both against the controller and also against the processor;
- the right to compensation from the controller or processor for material or non-material damage suffered as a result.

Contact the National Commission for Data Protection

NATIONAL COMMISSION FOR DATA PROTECTION

1, avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette
Phone.: (+352) 26 10 60 - 1 | Fax.: (+352) 26 10 60 - 29

Opening hours:
09.00 - 12.30 & 13.30 - 17.30

For questions or comments, please use the form available on **cnpd.public.lu**, "contact"- section or send an e-mail to **info@cnpd.lu**