Level 4

Governance 2.0: New processing – complaint – continuous improvement

Key words: impact assessment - continuous improvement - archiving - data of minors - storage - sufficient safeguards - one-stop shop - corrective measures (penalty) - data minimisation - further processing - direct complaint - complaint (CNPD)

Luxembourg House of Cybersecurity

CNPD National Commission for Data Protection Grand-Duchy of Luxembourg

Co-funded by the European Union

Update : 4th June 2024

Continuous Improvement (PDCA)

Taking into account the nature, scope, context and purposes of processing as well as the risks ofvarying likelihood severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. These measures shall bereviewed and updated wherenecessary (Art. 24 GDPR).

NEW PROCESSING, DEVELOP GOOD HABITS!

Purpose and further processing

In accordance with Article 5(1)(b) GDPR, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes.

This means that prior to any collection of data, the controller will have to precisely define the purpose(s) he/she actually wishes to pursue by collecting such data and may not subsequently use it for any other purpose. Consequently, an employer who decides to install a geolocation system for the sole purpose of protecting their vehicles against theft will not then be able to use it to monitor the working time of their employees. This would constitute another purpose for which the data were not initially collected and used and which was not brought to the attention of the employees.

Processing of data for a purpose other than that for which the data were collected may take place only if the new purpose is compatible with the initial one, in accordance with the principle of purpose limitation.

In order to determine whether or not a purpose is compatible, you must take into account the following (if the initial processing was not based on the consent of the data subject or on Union or national law adopted pursuant to Article 23 GDPR):

- Whether there is a link between the purposes for which the personal data were collected and the purposes of the intended further processing;
- The context in which the personal data was collected, in particular as regards the relationship between the data subjects and yourself;
- The nature of the personal data, in particular if the processing relates to special categories of personal data, pursuant to Article 9 of the GDPR, or if personal data relating to criminal convictions and offences are processed, pursuant to Article 10 GDPR;
- The possible consequences of the envisaged further processing for the data subjects;
- The existence of appropriate safeguards, which may include encryption or pseudonymisation.

What about children's consent?

If you collect data related to children, in particular through your commercial website (e.g. online games, social networks), it is necessary to obtain the consent of their parents or legal guardians. Information for users must be easy to understand and formulated in simple and clear terms.

Data minimisation principle

Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

Also known as the principle of necessity and proportionality, data minimisation means that you must only process data that is necessary (and not only useful) for the fulfillment of the purposes.

For more information:

The main principles

Data processing of minors

The consent of the data subject constitutes one of the legal bases or "conditions of lawfulness" on which the processing of personal data may be based.

The provisions concerning the conditions applicable to consent have been further developed by the GDPR, emphasizing its "freely given, specific, informed and unambiguous" nature. The data subject must therefore have a real choice of their parents or legal guardians. Information for users must be easy to understand and formulated in simple and clear terms.

For more information:

EDPB recommendation

Data protection impact assessment

If you have identified processing of personal data that may result in high risks to the rights and freedoms of data subjects, you must conduct a Data Protection Impact Assessment (DPIA) for each of these processing operations.

The data protection impact assessment makes it possible to:

- Develop a processing of personal data or a product that respects privacy,
- Assess the impact on the privacy of the data subjects,
- Demonstrate that the fundamental principles of the Regulation are respected.

The challenge is to assess data protection risks from the perspective of data subjects.

In accordance with Article 35(4) GDPR, the CNPD has drawn up a list of types of processing operations for which it considers that a data protection impact assessment is mandatory in all cases.

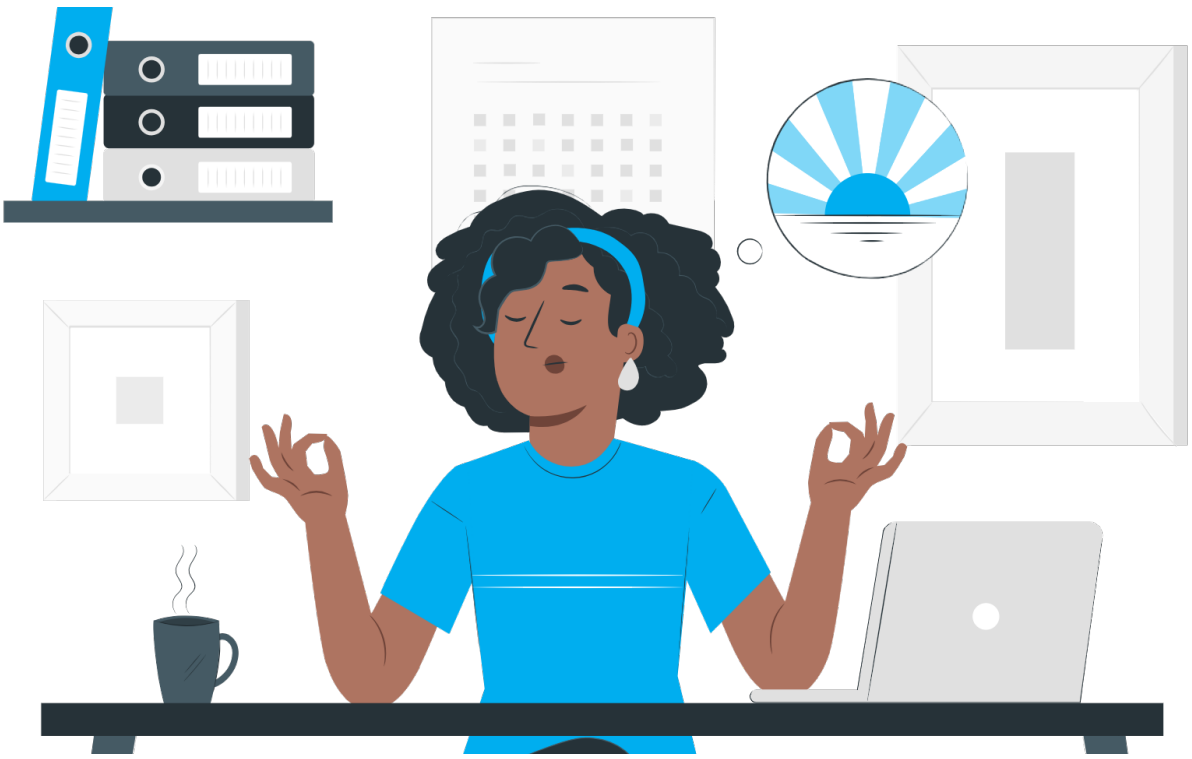
Reminder (Art. 35 and Art. 36 GDPR):

- The DPIA must be carried out before the processing takes place;
- The controller must carry out a pre-processing consultation with the CNPD for an opinion on the DPIA if the processing still poses a high residual risk to the rights and freedoms of individuals after measures to mitigate the risk have been put in place.

It should be stressed that the current list is not an exhaustive list of all types of processing operations requiring the performance of a DPIA. Thus, the absence of a type of processing operation on that list does not necessarily mean that a DPIA is not required. The list is limited to processing activities that will always require the performance of a DPIA. For processing activities not included in this list, data controllers should rely on Article 35(1) GDPR and the WP248 Guidelines of the Article 29 Working Party to assess the need for a DPIA.

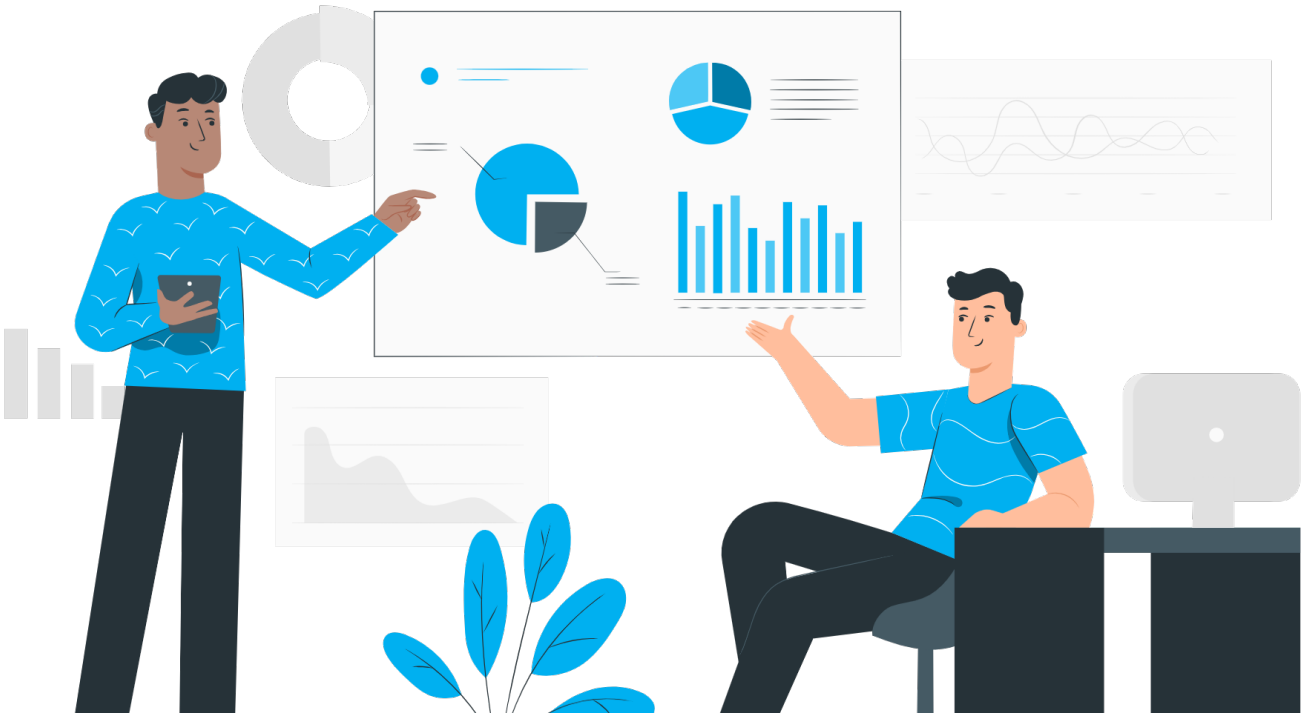
Learn more about :

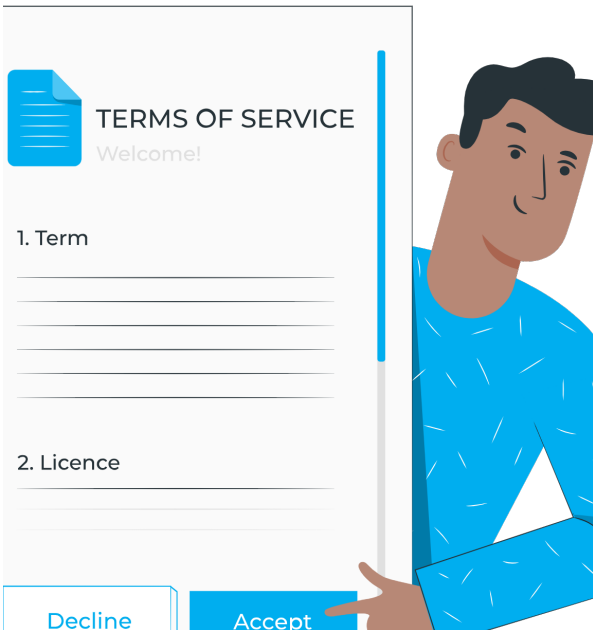
DPIA



List of processing operations for which a data protection impact assessment is required

1. Processing operations involving genetic data as defined in Article 4 (13) of the GDPR, in combination with at least one other criterion set out in the guidelines of the European Data Protection Board (hereinafter: EDPB), with the exception of health professionals who provide health services;
2. Processing operations that include biometric data as defined in Article 4 (14) of the GDPR for the purpose of identifying data subjects in combination with at least one other criterion of the EDPB Guidelines;
3. Processing operations involving the combination, correspondence or comparison of personal data collected from processing operations with different purposes (from the same or different controllers) - provided that they produce legal effects vis-à-vis the natural person or have a significant and similar impact on the natural person;
4. Processing operations which consist of or include regular and systematic monitoring of the activities of employees - provided that they may produce legal effects vis-à-vis employees or affect them a significant way;
5. File processing operations likely to contain personal data of the entire national population, provided that such a DPIA has not already been carried out as part of a general impact assessment in the context of the adoption of that legal basis;
6. Processing operations for scientific or historical research purposes or for statistical purposes within the meaning of Articles 63 to 65 of the Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection regulation;
7. processing operations consisting of systematic monitoring of the location of natural persons;
8. Processing operations based on the indirect collection of personal data in conjunction with at least one other criterion of the EDPB Guidelines where it is neither possible nor feasible to guarantee the right to information.





Sufficient guarantees from the processor

In order to ensure that the requirements of the General Data Protection Regulation are met in the context of processing carried out by a processor on behalf of the controller, where the controller entrusts processing activities to a processor, the controller should only use processors with sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, for the implementation of technical and organisational measures that will meet the requirements of this Regulation, including for the security of processing.

It should be made clear that the need to review processor agreements and adequate safeguards arises, in particular, in the event of a change of service provider.

In addition, the application by a processor of an approved code of conduct or an approved certification mechanism may serve to demonstrate compliance with the obligations of the controller.

Data storage and archiving

- Active base storage

This is the time needed to achieve the purpose (purpose of processing) for which the data were collected/recorded. For example, in a company, the data of an unsuccessful candidate will be kept for a maximum of 2 years (unless they request its erasure) by the Human Resources department.

In practice, the data will then be easily accessible in the immediate working environment for the operational departments responsible for this processing (e.g. the human resources department for recruitment operations);

- Intermediate archiving

Personal data are no longer used to achieve the objective set (‘closed files’) but are still of administrative interest to the organisation (e.g. management of any disputes, etc.) or must be kept in order to comply with a legal obligation (for example, billing data must be kept for ten years in accordance with the Commercial Code, even if the data subject is no longer a customer). The data may then be consulted on an ad hoc and motivated basis by specifically authorised persons;

- Final archiving

Because of their “value” and interest, some information is archived definitively and permanently.

Unlike active base storage, the last two steps are not systematically implemented. Their necessity must be assessed for each processing operation, and for each of these phases, the data will be sorted.

THE COMPLAINTS, WHO? WHAT? HOW?

To whom should complaints be addressed?

Controllers must enable the data subject to know to whom they should address their complaints under the rights provided for in the GDPR.

To this end, companies must provide information on the exercise of rights in simple and clear language at the time of data collection or, at the latest, within one month of collection.

In the case of the processing of personal data, the following information must be communicated by the controller to the data subject:

- The identity and contact details of the controller and, where applicable, the representative of the controller;
- Where applicable, the contact details of the Data Protection Officer (DPO).

Direct complaints

Data subjects may exercise their rights of access, erasure and rectification at any time directly with the controller as soon as the data concerning them are collected, stored, used or processed.

The information requested must be obtained free of charge. The controller may request additional information necessary to confirm the identity of the complainant, if the controller has reasonable doubts as to the identity of the complainant.

Find out more about :

Right to information

Prior steps taken by the complainant

Article 4 of the CNPD's complaint procedure provides:

'If the purpose of the request is to exercise the rights of the data subject conferred on him or her by Articles 12 to 22 of the GDPR and Articles 11 to 15 of the Law of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal matters and in matters of national security and the complainant has not himself or herself sought to exercise his or her rights directly with the controller in question, the CNPD shall send him or her an email or post informing him or her of the steps he or she must take, prior to any referral to the CNPD.'

Therefore, before lodging a complaint with the CNPD, the latter invites the data subjects to take the first step with the controller to enforce their rights (access, rectification, erasure, portability ...).

Find out more about :

The complaint procedure

Complaint to the CNPD

If the complaint to the controller has not been followed up (or if such a complaint proves difficult to make or even impossible in the circumstances), the data subject may contact the CNPD directly. One of its tasks is to deal with complaints from data subjects.

The CNPD may prohibit the processing of data in the event of non-compliance with the law. It may also order the deletion of data and refer the matter to the State Prosecutor. Penalties may be imposed for infringements.

It is strongly recommended that the data subjects submit the complaint using the online form of the CNPD. The use of this form will allow an accelerated processing of their claim.

The Complaints Department of the CNPD examines, in the light of the legal texts on data protection, whether the CNPD is materially and territorially competent to deal with the complaint.

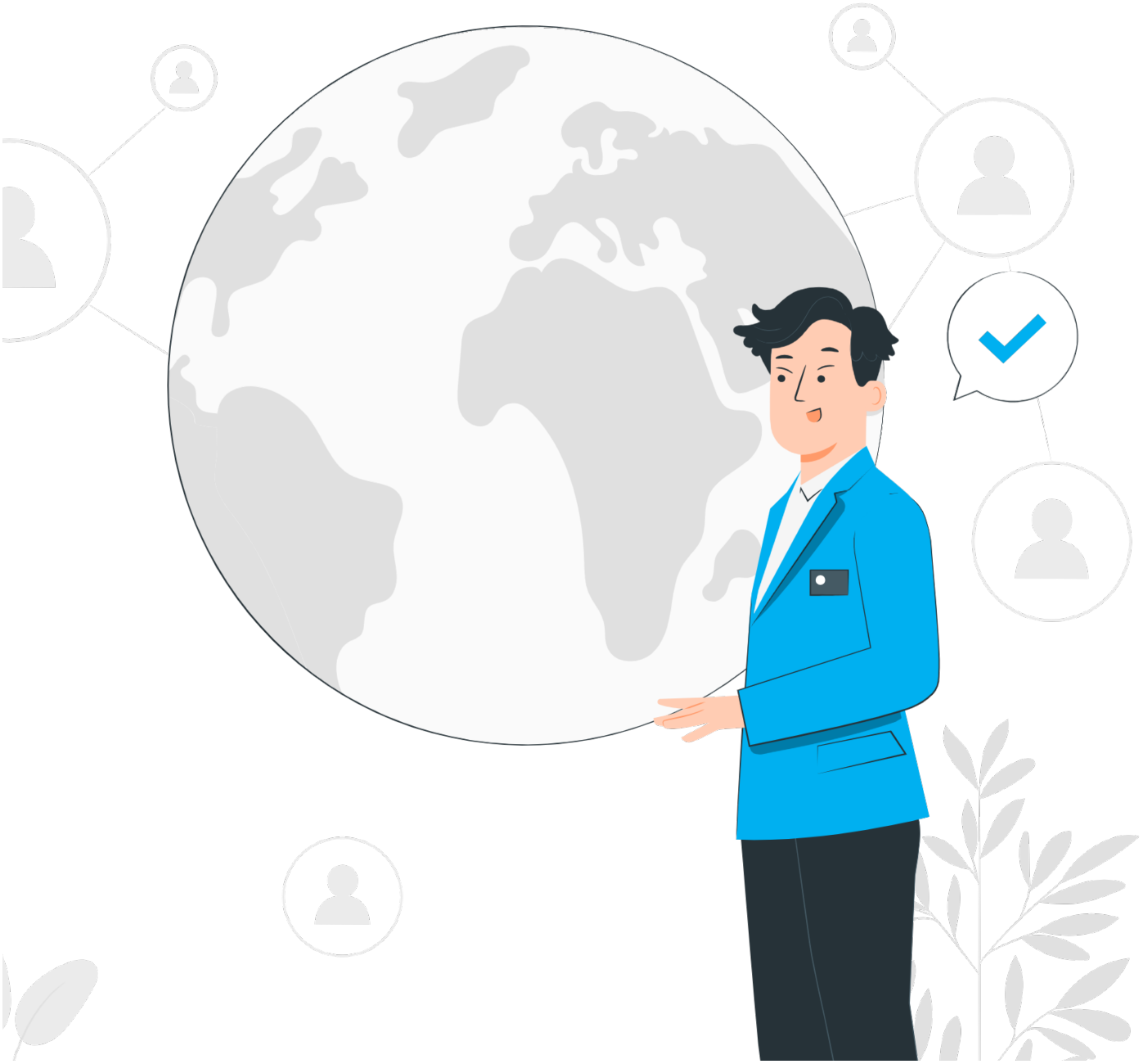
During the complaint procedure, the CNPD examines whether a complaint is justified, i.e. whether or not the facts alleged by the complainant relating to the processing of personal data are likely to constitute a breach of the applicable data protection legislation. Where the CNPD considers that the processing of the data at issue would indeed be contrary to the law, it will endeavour to remedy the situation without having to resort to binding measures available to it under its powers conferred on it by law.

One-stop-shop (European complaints)

Under the GDPR, supervisory authorities have a duty to co-operate in cases with a cross-border component to ensure the consistent application of the GDPR. Under this one-stop-shop mechanism, the lead supervisory authority is in charge of preparing draft decisions and works with the other supervisory authorities concerned to reach a consensus.

For more information:

CNPD website



NOUVEAUX TRAITEMENT, AYEZ LES BONS REFLEXES !

Corrective measures

Each supervisory authority (including the CNPD) has the power to adopt all of the following corrective measures:

notifying a controller or processor that the planned processing operations are likely to infringe the provisions of this Regulation;

reprimanding a controller or processor where the processing operations have resulted in a breach of the provisions of this Regulation;

ordering the controller or processor to comply with requests made by the data subject to exercise his or her rights under this Regulation;

ordering the controller or processor to bring the processing operations into compliance with the provisions of this Regulation, where appropriate, in a specific manner and within a specified period of time;

ordering the controller to communicate a personal data breach to the data subject;

imposing a temporary or permanent restriction, including a prohibition, on processing;

ordering the rectification or erasure of personal data or the restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such measures to the recipients to whom the personal data have been disclosed pursuant to Articles 17(2) and 19;

withdrawing a certification or order the certification body to withdraw a certification issued under Articles 42 and 43, or order the certification body not to issue a certification if the requirements for certification are not or no longer met;

imposing an administrative fine pursuant to Article 83, in addition to or in place of the measures referred to in this paragraph, according to the specific characteristics of each case;

ordering the suspension of data flows to a recipient located in a third country or to an international organisation.

Source: Art. 58(2) GDPR

PROCESSING PHOTOS IN ACCORDANCE WITH APPLICABLE LAWS!

Legal basis within the meaning of Article 6 GDPR

Most of the time, the processing of photos will be based on the consent of the data subject. Consent must be "freely given, specific, informed and unambiguous". The data subject must therefore have a real choice. For minors, the legal representatives must give their consent.

Photo processing may also be based on other conditions of lawfulness (e.g.: public interest, performance of a contract).

For example, a photographer may rely on the condition of lawfulness relating to the performance of a contract when taking ID photos or when hired for a photo shoot.

Public authorities may invoke the public interest or the vital interest of the data subject when publishing photos, such as of missing persons.

Other applicable laws

The "image rights" are regulated not only by the GDPR but by a series of other laws and case-law:

- Art. 8, 10, 17 European Convention on Human Rights
- Art. 7, 8, 54 Charter of Human Rights
- Art. 16 Treaty on the Functioning of the European Union
- Art. 6, 85 GDPR
- Art. 11(3), 24 Luxembourg Constitution
- Law of 11 August 1982 concerning the protection of privacy
- Amended Law of 8 June 2004 on freedom of expression in the media
- Amended Law of 18 April 2001 on copyright, related rights and databases
- Amended Law of 10 August 1992 on the protection of young people (minors: Art. 38)
- Art. 383, 383bis, 385 Criminal Code
- Art. 1382 et seq. C. civ. / injunction
- The case-law: It is settled case-law that "any individual has an exclusive right over their image and the use made of it and may oppose a dissemination not permitted by them". Thus, it has been held that 'an individual's right to their private image is absolute and that anyone can object to the publication of their likeness without permission'.
- The relevant case-law holds that a person who gives their consent for the taking of photos does not necessarily give it for publication or dissemination.Therefore, a separate consent must be obtained for these purposes.

For more information :

Guidance from the CNPD

Disclaimer:

This document is a summary sheet of the explanations provided under the DAAZ tool to illustrate the answers. The content is provided for informational purposes only and should not be construed as a complete and exhaustive statement of the topics discussed. The content in no way engages the responsibility of the CNPD. In case of conflict between this document and the guidelines published on the CNPD website, only the guidelines prevail.