Level 2

DESIGN: GDPR PROCEDURES, ROUTINES AND DOCUMENTS

Key words: badge, meal voucher, consent, personal data of employees, right of access, right to erasure, geolocation, images, photos, transparency, video surveillance

Luxembourg House of Cybersecurity

CNPD National Commission for Data Protection Grand-Duchy of Luxembourg

Co-funded by the European Union

Update : 4th June 2024

HOME THE "TRANSPARENCY"

Controller

In the context of the employment relationship, the controller is in principle the employer. Thus, a specific staff member or department will in principle not be the controller, but will act on behalf of the employer, who is responsible for compliance with the GDPR.

Good to know:

The delegation of staff, as a representative body of employees, is to be regarded as separate from the employer and therefore a separate controller.

Processor

Good to know:

A processor may not process the data entrusted to it by a controller for its own purposes. Otherwise, he or she becomes the controller for the processing carried out in this way, with all the responsibilities attaching to it.

Good to know:

The parties cannot freely agree in the contract on their respective qualities under the GDPR. Qualifications as a controller or processor must be based on a factual analysis for each data processing operation.

The processing of personal data of employees

Since the recruitment process and after the end of the employment relationship, the employer is faced with a significant number of cases where it will have to apply data protection rules.

An employer is often required to collect personal data, for example when a candidate sends him or her his or her application file, when an employee provides him or her with his or her bank details so that he or she can pay his or her salary, during the annual professional appraisals of his or her employees, or in order to reimburse travel expenses to one of his or her employees.

It is up to the employer to determine, before any processing of personal data and in the light of the specific context, which basis(s) of lawfulness is (are) the most appropriate and can justify the envisaged processing.

It is still up to the employer, as controller (see insert "Good to know"'), to document its compliance with the GDPR (principle of 'accountability'). This documentation will be necessary for the controller, in particular in the event of control by the CNPD or when the data subjects make use of their rights (see below).

Special categories of data ("sensitive data"):

Particular vigilance is necessary in the event of the processing of so-called "sensitive data". These are special categories of data within the meaning of Article 9 GDPR, namely data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sexual life or sexual orientation of a natural person.

For example, the information that an employee is on maternity leave is to be regarded as "sensitive data", because that information is data relating to the health of the data subject. The same applies to the pre-employment medical certificate, which, by informing the employer whether or not an employee is fit for a given post, contains data relating to the employee's health.

Similarly, information that an employee is a member of a trade union constitutes "sensitive data".

Transparency requirement

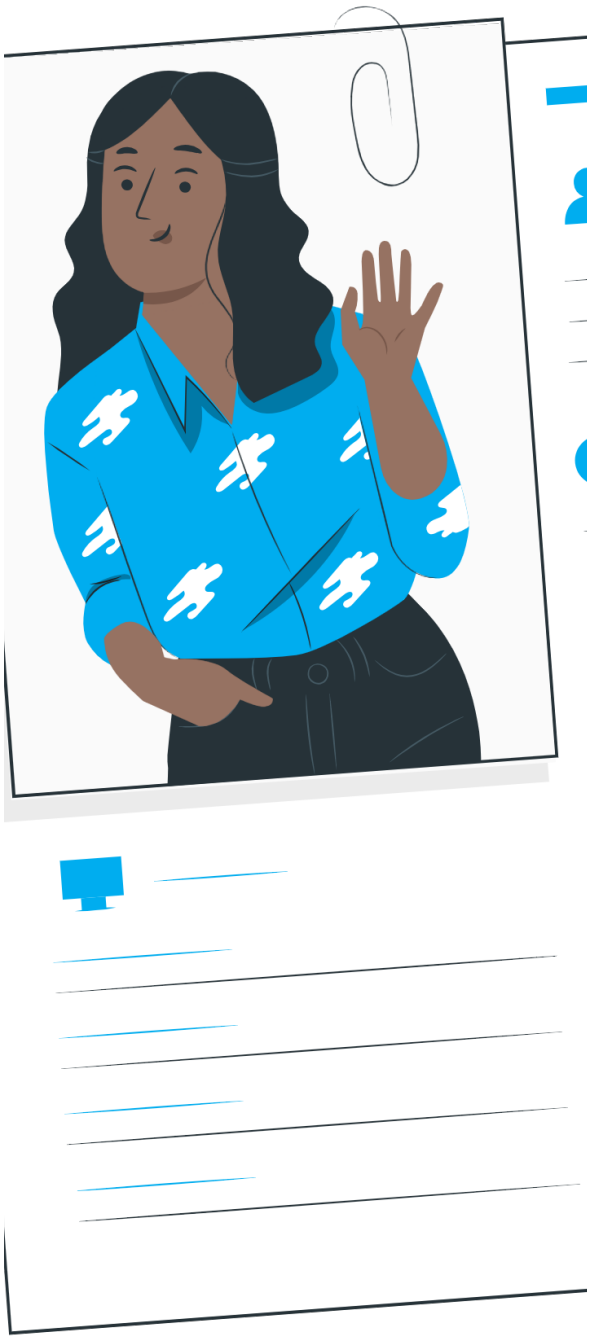
In accordance with the principles of transparency and fairness, data subjects (e.g. candidates and employees) must receive certain information concerning the processing of their data by the employer, in order to enable them to understand why the data are collected, the use that will be made of them, and the rights they have to monitor the lawfulness of the processing carried out by the employer.

Characteristics of the information to be given

Any controller shall be obliged to inform the data subjects individually of the processing of personal data which it carries out.

In accordance with Article 12(1) of the GDPR, the provision of information to data subjects and communications addressed to them must be carried out in a 'concise, transparent, intelligible and easily accessible manner, in clear and plain language'.

The word 'providing' is crucial here and means that the controller must take concrete steps to transmit the information in question to the data subject or to actively direct the data subject to the location of that information (e.g. by means of a direct link, a QR code, etc.).



GOOD TO KNOW:

In accordance with the principle of accountability, the employer must at all times be able to demonstrate that it has provided the required information to the data subject.

The employer should also take into account any sectoral obligations or obligations deriving from other legislation, such as the obligation to provide information on surveillance at the workplace deriving from Article L. 261-1 of the Labour Code.

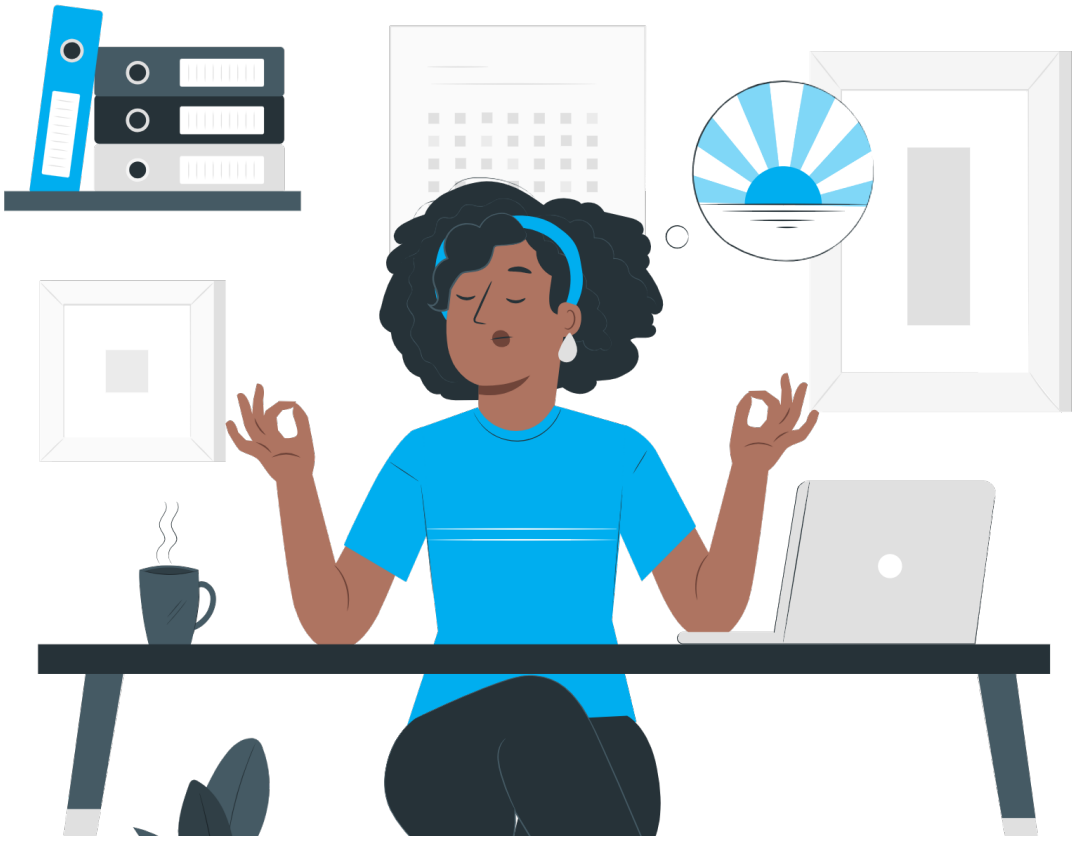
The content of the information

The employer must provide employees with all the information listed in Article 13 GDPR (or Article 14, if the data are not collected directly from the data subject), under the conditions laid down in Articles 12, 13 and 14 GDPR.

The information to be provided must enable the data subjects to understand the scope of the processing operations carried out by the employer and must be adapted to the specificities of those operations. The employer must, inter alia, state:

- the purposes of the processing for which the personal data are intended and the legal basis for the processing (i.e. the condition of lawfulness on which the processing is based); if so-called 'sensitive' data are processed, the exception in Article 9 of the GDPR that applies, and if judicial data within the meaning of Article 10 of the GDPR are processed, the legal provisions under which the processing is carried out;
- where the processing is based on the legitimate interest, a description of the legitimate interests pursued by the controller or by a third party;
- where the data are collected directly from the data subject, whether the requirement to provide the personal data has a regulatory or contractual nature or whether it is a condition for concluding a contract and whether the data subject is required to provide the personal data, as well as the possible consequences of not providing such data (e.g. the national identification number);
- where the data are not collected directly from the data subject, the source from which the personal data originate and, where applicable, whether or not they originate from publicly available sources (e.g. a social network).

The CNPD recommends that employers ensure that the data processing operations listed in the information notice correspond to the processing operations listed in the processing register.



In what form should the information be provided ?

Information and communications should, in principle, be addressed to the data subjects in writing. They may also be accompanied by other means to facilitate the understanding of data subjects.

In addition, the GDPR requires that information be "provided" to data subjects.

The employer could, for example, fulfil its obligation to provide information by providing the information required in an annex to the employment contract or by inserting in the employment contracts a clause relating to the processing of personal data carried out in the context of personnel management provided that the clause in question is clear, complete, explicit and clearly differentiated from the other terms of the contract.

The arrangements for providing and presenting this information must be adapted to the circumstances of the collection and processing of the data and must, in particular, enable the data subjects to understand the reason for the collection of the various data concerning them, the processing which will be carried out and their rights. Thus, depending on the conditions of the processing, it might be useful for the controller to adopt a multi-layered approach to the communication of information to data subjects.

The first level of information should include the most important information, namely the details of the purpose of the processing, the identity of the controller, a description of the rights of data subjects and a mandatory reference to the second level of information where data subjects can find all information, for example by means of a QR code or a direct link. Depending on the processing, the employer should also include in the first level information on the processing that will have the greatest impact on the data subject and on any processing that might surprise him or her. Therefore, the data subject should be able to understand from the information provided at the first level/modality what the consequences of the processing in question will be for him/her.

Example

In order to protect the company's assets and secure access to the building, the employer wishes to install a video surveillance system to monitor the premises where its employees work. He shall install at the main entrance door of the building a pictogram bearing the words '24-hour video surveillance' and shall also inform the staff delegation thereof.

In the present case, the employer did not comply with the information requirements imposed by Article 13 of the GDPR. Indeed, the mere information of the Staff Delegation does not ensure that employees have been individually informed of the precise elements of Article 13 GDPR. Furthermore, the pictogram referring to '24-hour video surveillance' does not contain all the required elements.

In this context of the processing of personal data by means of a video surveillance system, the employer could use two levels of information. The first level should generally include the most essential information (details of the purpose of the processing, the identity of the controller, the existence of data subjects' rights and a mandatory reference to the second level of information, for example by means of a QR code or a direct link). The CNPD makes available on its website a first-level billboard template.

The second level of information, i.e. all the information required under Article 13 GDPR could be provided by other means, such as a copy of the privacy policy sent by email to all employees.

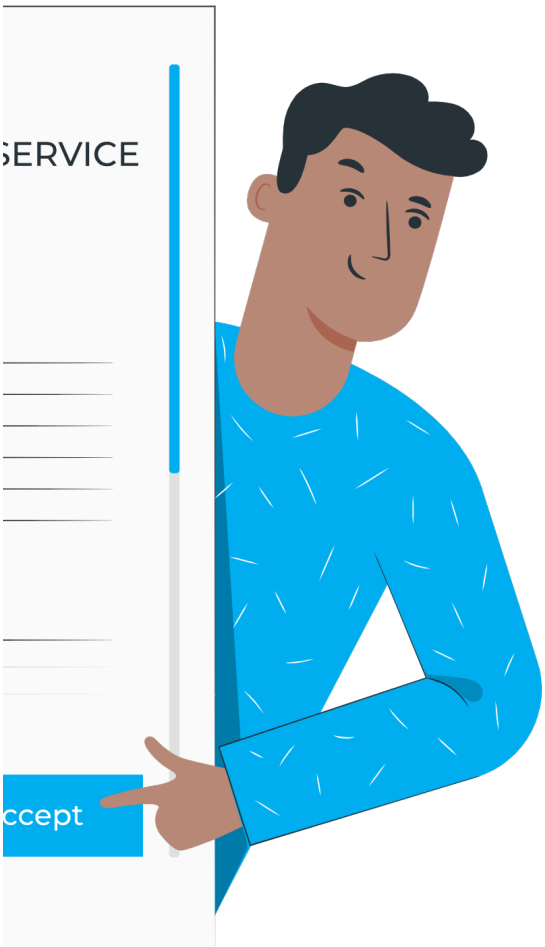
Good to know:

It should be pointed out in this context that the mere signature of an information sheet or employment contract by the employee can at most be regarded as an acknowledgement of receipt enabling the employer to document that it has indeed provided the required information to the employee, but cannot in any event constitute valid consent of the employee to the processing of data by his employer within the meaning of the GDPR.

Good to know:

A mere reference to the GDPR is not in line with the GDPR's transparency requirements. The employer must provide specific information about the treatments it carries out.

In accordance with the principle of accountability, it is not the CNPD's task to analyse or validate the employer's information notice a priori.



When should the information be provided?

The timing of the provision of information depends on the form of collection. However, regardless of the form of collection, the timely provision of information "...is an essential element of the obligation of transparency and the obligation to treat data fairly."

In case of direct collection, the information must be provided at the latest at the time of collection from the data subject, for example when a candidate fills in a form made available by the employer. The employer must therefore ensure that the (future) employee has received the required information as soon as the data are collected.

In the case of indirect collection, the information must be provided as soon as possible (in particular during the first contact with the data subject), unless exceptions apply.

The employer should document the provision of the information for evidentiary purposes such as by signing a receipt certifying the provision of the information.

For more information:

Articles 12, 13 and 14 GDPR, Fact Sheet and video clip of the CNPD on the right to information.

SOME GDPR "ROUTINES" OF THE PROFESSIONAL WORLD

Purpose

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.

For example, surveillance by video cameras may have the following purposes:

- Secure access to the building;
- Ensure the safety of staff and customers;
- Detect and identify potentially suspicious or dangerous behaviour likely to cause accidents or incidents;
- Accurately identify the origin of an incident;
- Protecting assets (buildings, facilities, equipment, merchants, cash, etc.);
- Organising and supervising the rapid evacuation of persons in the event of an incident;
- To be able to alert the emergency, fire or law enforcement services in good time and to facilitate their intervention.

Before installing a video surveillance system, the controller must define precisely the purpose(s) it wishes to achieve by using such a system, and may not subsequently use it for any other purpose.

Protection of Employees' Property and Behaviour

The CNPD considers that video surveillance should not be used to observe the behaviour and performance of the controller's staff members outside the purposes for which it was set up.

Thus, an employer has the right to use images of an employee who commits theft of goods and which come from a video surveillance system used for the purpose of protecting property. However, he does not have the right to take action against an employee where, to the employer's liking, the employee talks too much with a client or colleague at work and that conduct is recorded by the video surveillance system. This would constitute a misuse of purpose prohibited by the GDPR.

Example: *cash register of a shop*

The purpose of camera surveillance of a cash register in a shop may be to protect the controller's assets against acts of theft committed by its employees or by a customer/user and to ensure the safety of its staff. However, in order not to infringe the privacy of employees, the camera should be configured so that employees behind a cash desk are not targeted, by directing its field of view towards the cash desk itself and the front of the counter, i.e. the waiting area of customers in front of the counter, in order to allow the identification of perpetrators, for example.

Example: *access point*

Cameras intended to monitor an access point (entrance and exit, threshold, stairway, door, canopy, hall, etc.) must have a field of view limited to the area strictly necessary to visualise the persons preparing to access it; those filming external accesses shall not cover the entire width of any pavement running alongside the building or adjacent public roads. Similarly, exterior cameras installed in or around a building must be configured in such a way that they do not capture the public road or the approaches, entrances, accesses and interiors of other neighbouring buildings which may fall within their field of vision. Depending on the configuration of the premises, it is sometimes impossible to install a camera that does not include in its field of vision part of the public road, approaches, entrances, accesses and interiors of other buildings. In such a case, the CNPD considers that the controller must implement masking or blurring techniques in order to limit the field of vision to its property.

The meal voucher

The amended Grand-Ducal Regulation of 29 December 1986 implementing Article 115, number 21 of the Income Tax Act provides in this context in Article 2(2) that "meal vouchers must, apart from the designation of the issuing employer, their value and purpose, bear a distinguishing sign identifying the user."

In this context, the CNPD considers that the use of the national identification number ('ID number') for the purpose of issuing meal vouchers (digitalised or not) appears to be incompatible with the principle of data minimisation.

The badge device

The GDPR does not prohibit the display of surnames and first names on badges, but requires that appropriate measures be put in place with regard to these personal data.

The principles of data minimisation and proportionality must be taken into account when creating badges, ensuring that only information that is strictly necessary for the objective pursued is displayed.

For example, displaying only the first name, using codes or initials can be effective measures to protect the privacy of individuals while allowing their identification when necessary.

With regard to photography, in certain cases, the employer may require a photograph to be taken in order to produce an access badge which is necessary for security reasons. On the other hand, it is not permissible to require the publication of a photo on an internal network, on the internet or in a paper publication.

Good to know:

The photo taken for the production of an access or legitimation badge (photo printed on the badge so that visual identification is possible) cannot automatically be reused for the internal organisation chart or internal messaging.

Image and photo taking

As regards image rights, it is settled case-law that 'everyone has an exclusive right over their image and the use made of it and may oppose unauthorised dissemination by them. Thus, 'everyone may oppose the publication of their features without authorisation'.

Similarly to consent in the context of data protection, consent in terms of image rights must be free, certain and specific. This means that, in principle, the employee must be able to oppose or consent separately to the shooting or transmission of an image, and to the dissemination on the various publication media (website, internal network, paper media). The employee remains in control of his or her image and may in principle refuse to take 'untimely and impromptu photos' and also withdraw his or her consent for the publication of a specific photo.

However, since personal data are any information relating to an identified or identifiable natural person, a photograph is therefore personal data.

Thus, as regards the protection of personal data, one of the conditions to be met for consent to be valid – which derive from Article 4. 11) GDPR – is that it was freely given by the data subject. Given the dependence and imbalance of powers that may exist in 'employer-employee' relationships, employees are only very rarely able to refuse or revoke their consent without fear of adverse consequences. In these circumstances, consent cannot be considered to be freely given.

Finally, the disclosure of personal data such as a photo in an internal network to employees does not appear to be in line with the data minimisation principle set out in Article 5(1)(c) GDPR. Therefore, the photograph of the employee does not seem necessary in most working contexts in view of the objective of setting up an internal network.

To sum up: Apart from certain specific cases, the majority of employment relationships do not justify taking photographs of employees and entering them in the company's internal mailbox.

For more information:

Video surveillance guidelines published on the CNPD website

Geolocation

Legal basis

Any processing of personal data must be based on one of the conditions of lawfulness exhaustively listed in Article 6(1)(3) GDPR. In the context of a geolocation system set up by an employer vis-à-vis its employees, a valid condition of lawfulness could be that the processing is necessary for the purposes of the legitimate interests of the controller, unless the interests or fundamental rights and freedoms of the geolocated person(s) prevail (Article 6(1)(f) GDPR).

Furthermore, in the event that the installation of a device for the geolocation of employees' vehicles is imposed on the employer by a rule of national or European law (e.g. legislation applicable in the field of national and international road transport), the condition of lawfulness of Article 6(1)(c) of the GDPR could apply.

For the reasons explained above (inclusion on the free nature of consent), consent does not constitute an appropriate basis for lawfulness in relation to the geolocation of employees.

Working hours

Vehicle geolocation systems made available to employees allow employers to track the movements of their employees over time and space. The democratisation of these systems makes their use increasingly frequent in the business world. However, as the use of such devices involves the processing of personal data, it raises certain data protection issues and entails risks to the privacy of employees. Thus, geolocation exposes employees to the risk of being monitored in real time by their employer outside working periods, or to the risk that the geolocation system is used by the employer for purposes other than those for which it was installed.

The processing of employees' personal data resulting from the use of a video surveillance system for the purposes of time control does not appear to be necessary when there are less intrusive means of controlling employees' working hours and time spent by the employer.

Indeed, controlling working hours by badges via a clocking-in system is more effective and more protective of the privacy of employees.

For more information :

"Geolocation of vehicles" guidelines published on the CNPD website

RESPECT INDIVIDUAL RIGHTS

Complément : contexte professionnel

Complement: professional context

In order to enable the exercise or defence of legal rights, the GDPR provides for exceptions in the exercise of the various rights conferred by the text. Within this strict framework of exercising or defending legal rights, it is permitted to process sensitive data or not to respond favourably to a request for the exercise of the right to erasure or the right to object to processing.

However, as regards the right of access, the employer must respond favourably to the request for the right of access of an employee with whom he is in conflict (e.g. dismissal), even if this information may be used against them; otherwise, he will be in breach of the GDPR. The employer must not ask the employee to give reasons for his or her request. The employer must nevertheless verify that this request for a right of access does not affect the rights of third parties or business secrecy. The right of access is not an absolute right (see below).

For more information :

EDPB Guidelines on the right of access

Right of access and right of third parties

Article 15 GDPR does not distinguish personal data according to their origin, in this case according to whether the data have already been provided in the past to the controller by the data subject himself or herself (e.g. at the time of signing an employment contract). The former employer must therefore provide these documents to the former employee.

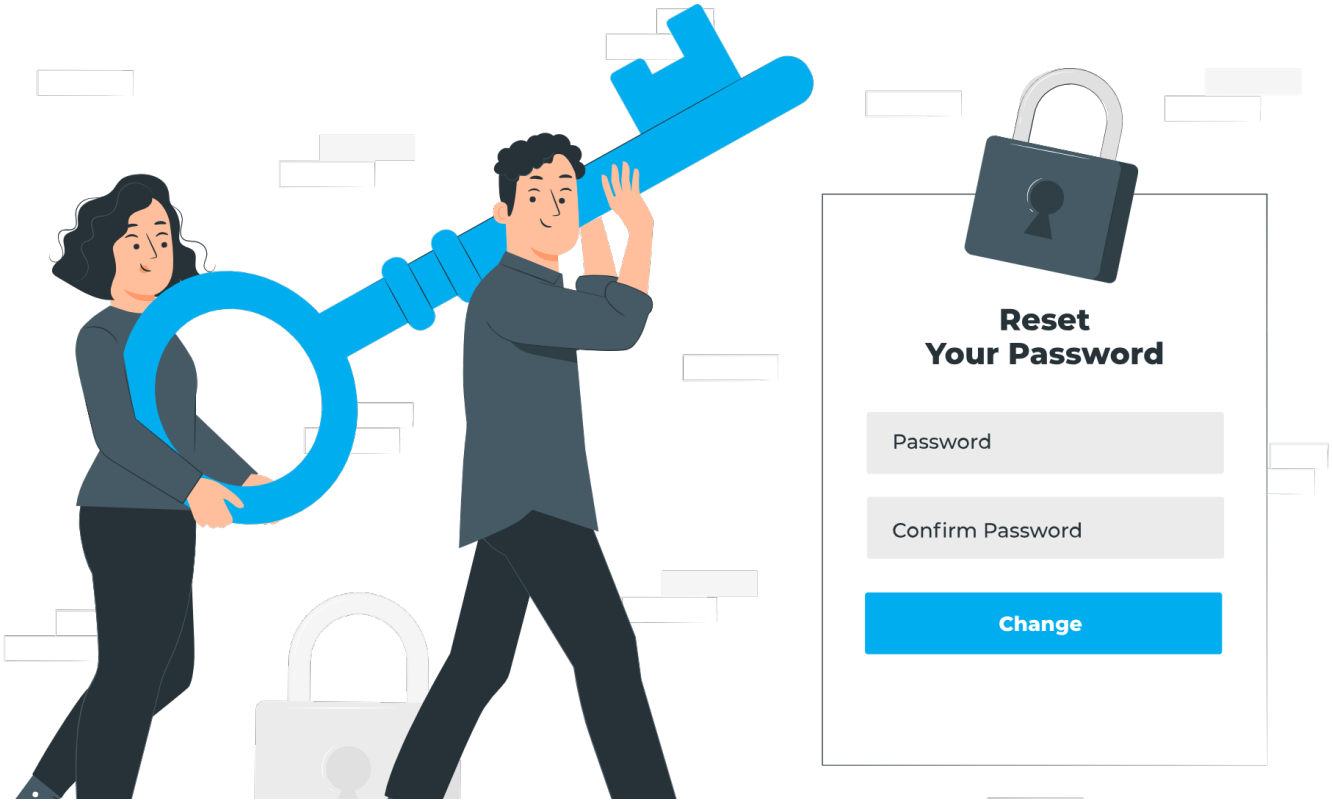
With regard to e-mail exchanges, it is suggested to ask the data subject to specify which e-mails are covered by his/her request (e.g. according to the date of sending or receiving, or according to the recipient or sender of the e-mail). The CNPD then recommends that particular care be taken to avoid the communication of emails that infringe the rights and freedoms of others.

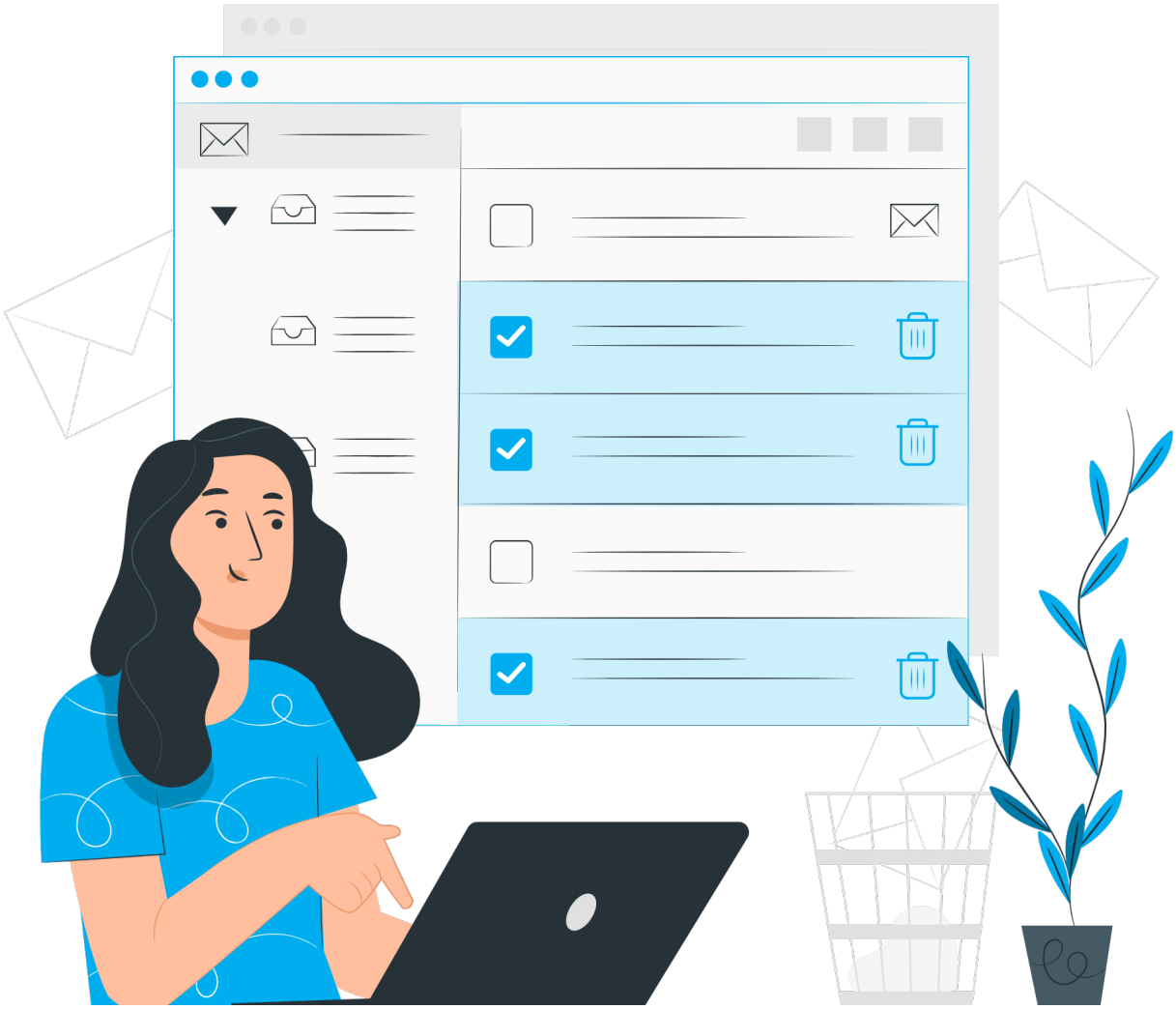
To this end, the controller should distinguish between e-mails, for example, according to their nature: emails marked as 'private' or 'personal' (insofar as the former employer would still have it), those concerning exclusively the relationship between the data subject and his or her employer (in particular for the purposes of human resources management), and finally those sent or received by the data subject in his or her capacity as an employee, that is to say in the context of his or her professional activity and therefore made in the name and on behalf of the employer. While the latter category of email is likely to infringe the rights and freedoms of others, in this case the employer, the communication of private or human resources emails seems less problematic in terms of potential infringement of the rights and freedoms of others.

As regards internal documents in which only the surname and first name of the former employee appear, it should be remembered that just because his surname and first name appear in such documents, this does not automatically mean that all the information contained in those documents is to be regarded as personal data concerning the former employee.

For more information :

Factsheet and video clip of the CNPD on the right of access.





Right to erasure and employee/ employer litigation

The right to erasure exists but is not an absolute right.

In fact, in accordance with Article 17(3) of the GDPR, it does not apply to the extent that such processing is necessary: for the exercise of the right of freedom of expression and information; to comply with a legal obligation which requires processing under Union or Member State law to which the controller is subject, or to perform a task carried out in the public interest or in the exercise of official authority vested in the controller; on grounds of public interest in the field of public health, in accordance with points (h) and (i) of Article 9(2) and Article 9(3); for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), in so far as the right referred to in paragraph 1 is likely to render impossible or seriously jeopardise the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims. In addition, it is important to be mindful of the rights of other persons who may be affected in the context of a request for erasure.