Deliberation 2019-160 of November 21, 2019 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Friday April 17, 2020 of personal data used for personnel management purposesThe National Commission for Computing and Liberties,

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Having regard to the labor code;

Considering the civil code, in particular its article 9;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms;

Having regard to Laws No. 83-634 of July 13, 1983 on the rights and obligations of civil servants, No. 84-16 of January 11, 1984 on statutory provisions relating to the State civil service, No. 84-53 of January 26, 1984 laying down statutory provisions relating to the territorial public service, and no. 86-33 of 9 January 1986 laying down statutory provisions relating to the hospital public service;

Having regard to Decree No. 2011-675 of June 15, 2011 relating to the individual file of public officials and its management on electronic media;

Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to the decree of 21 December 2012 relating to the composition of the individual file of public officials managed electronically,

After having heard Mr. Alexandre LINDEN, Commissioner, in his report and Mrs. Nacima BELKACEM, Government Commissioner, in her observations;

Adopts the reference system relating to the processing of personal data implemented for the purposes of personnel management, which will be published in the Official Journal of the French Republic.Appendix

REPOSITORY

FRAMEWORK RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED FOR PERSONNEL

MANAGEMENT PURPOSES

Adopted on November 21, 2019

1. Who is this reference for? This reference is intended for private or public bodies, regardless of their legal form, and provides a framework for the implementation of their current personnel management processes.

For the purposes of this standard, the terms: persons employed, effective personnel, human resources or human resources, are considered to be synonyms and designate all permanent or temporary employees of the employer, regardless of their status, type or length of contract, their level of remuneration. The provisions of this reference document cover in particular employees, civil servants, trainees, temporary workers, etc., who are part of the workforce of the employing body.

Organizations implementing personnel management processing must ensure compliance:

- the provisions of the general data protection regulations (GDPR) as well as those of the amended law of 6 January 1978 (LIL);

- to all other applicable rules such as labor legislation, texts governing the public service, collective agreements, etc.

2. Scope of the standard This standard aims to provide public and private organizations implementing day-to-day human resources (HR) management processing with a tool to help them comply with data protection regulations. of a personal nature. It covers the processing commonly implemented by employer organizations in the context of the management of their personnel.

It is therefore not intended to apply to the processing implemented in particular by trade unions, employee representative bodies, or occupational medicine services.

Due to their sensitivity, this reference system is not intended to regulate: - HR management processing involving the use of innovative tools such as psychometrics (i.e. techniques for quantifying personality aspects), algorithmic processing of purposes including profiling, or so-called Big Data processing, which will be treated separately;

- processing having as its object or effect the individual control of the activity of the employees.

Compliance with this standard enables organizations to ensure that the data processing implemented in this context complies with the principles relating to data protection.

Organizations that deviate from the reference system with regard to the particular conditions relating to their situation must be able to justify the existence of such a need, then take all the appropriate measures to guarantee the compliance of the

processing with the regulations in regarding the protection of personal data.

The repository is not intended to interpret the rules of law other than those relating to the protection of personal data. It is up to the players concerned to ensure that they comply with the other regulations which may also apply.

This reference also constitutes an aid to the realization of an impact analysis relating to data protection (DPIA), in the event that this is necessary.

To carry out an impact study, the data controller may also refer to the methodological tools offered by the CNIL on its website.

Organizations will thus be able to define the measures to ensure the proportionality and necessity of their processing (points 3 to 7), to guarantee the rights of individuals (points 8 and 9) and to control their risks (point 10 ). To this end, the organization will rely on the CNIL guidelines on DPIA. If the organization has appointed one, the data protection officer (DPD/DPO) must be consulted.

3. Objective(s) pursued by the processing (purposes) The processing implemented must meet a specific objective and be justified with regard to the missions and activities of the organisation.

Personnel management processing can be implemented for the following purposes:

a) Recruitment;

b) Administrative management of personnel;

c) Management of remuneration and completion of related administrative formalities;

d) Provision of staff with professional tools;

e) Organization of work;

f) Career and mobility monitoring;

g) Training;

h) Keeping of mandatory registers, relations with staff representative bodies;

i) Internal communications;

j) Management of social benefits;

k) Carrying out audits, managing litigation and pre-litigation.

The information collected for one of these purposes cannot be reused to pursue another objective that would be incompatible with the initial purpose. Any new use of data must indeed respect the principles of protection of personal data. The processing

implemented must not give rise to interconnections or exchanges other than those necessary for the fulfillment of the purposes set out above.

4. Legal basis(s) of the processing When processing pursues several purposes, the controller must determine the most appropriate legal basis for each of them (art. 6.1 of the GDPR).

It is up to the data controller to determine these legal bases before any processing operation, after having carried out a reflection, which he can document, with regard to his specific situation and the context.

Having an impact on the exercise of certain rights, these legal bases are part of the information that must be brought to the attention of the persons concerned.

In order to help the organizations in this analysis, this reference system presents the different applicable legal bases, then proposes, for information purposes, a choice of legal base for each purpose in a table.

Also, the most frequently mobilized legal bases in the context of human resources management are: - compliance with a legal obligation incumbent on the organization, imposing the implementation of processing within the framework of the management personnel (e.g. obligations related to the nominative social declaration (DSN) or the keeping of a single personnel register);

- the execution, either of a contract to which the data subject is a party, or of pre-contractual measures taken at his request. cannot as such constitute the legal basis for the processing of data of a person who is not himself a party to it.- the achievement of the legitimate interest pursued by the organization or by the recipient of the data , subject to not disregarding the interest or the fundamental rights and freedoms of the data subject;

- the performance of a task in the public interest or in the exercise of official authority vested in the controller. In certain exceptional cases, the following legal bases may also be invoked in the HR context:- the free, specific, informed and unequivocal consent of the person concerned.

Note: employees are only very rarely able to freely give, refuse or revoke their consent, given the dependence that arises from the employer/employee relationship. They can only give their free consent if the acceptance or rejection of a proposal has no consequences for their situation. Examples: the processing carried out in the context of recruitment operations cannot be based on the consent of candidates, since a refusal on their part could affect their chances of obtaining employment (or certain types of employment).

Conversely, the recording of a promotional clip in a workspace showing identifiable employees may be based on their consent

when the persons concerned have the choice of whether or not to appear in these recordings, and provided that the choice made has no impact on them (in particular with regard to working conditions, remuneration, advancement, etc.).

For an overview of the different legal bases, see the opinion of the former G29, now European Data Protection Board (EDPS) No. 06/2014 on the notion of legitimate interest pursued by the data controller. processing of data within the meaning of Article 7 of Directive 95/46/EC. most common cases.

Of course, these elements must be adopted to the specific situation of each organization concerned. Thus, for example, depending on whether the organization in question is in the private or public sector, certain processing operations that nevertheless serve the same purpose (for example, those related to the recruitment of staff) may be based on different legal bases (legitimate interest in the private sector, performance of a mission of public interest in the public sector).

For more advice on the method to follow, you can also refer to the article Lawfulness of processing: the main points on the legal bases provided for by the GDPR, published on the CNIL website.

Processing activities

Purposes

Possible legal bases

(subject to justified different choices)

by a specific context)

Recruitment

Processing of applications (CV and cover letter) and management of interviews

- Pre-contractual measures

Constitution of a CV-library

- Legitimate interest

Administrative management

Staff

Management of the professional file of the employees, kept in accordance with the legislative and regulatory provisions, as well as the statutory, conventional or contractual provisions which govern the interested parties.

- Execution of the contract

Production of statistical reports or lists of employees to meet administrative management needs.

- Legitimate interest

Management of internal directories and organizational charts.

- Legitimate interest

Management of individual allocations of supplies, equipment, vehicles and payment cards.

- Legitimate interest

Management of professional elections.

- Legal obligation

Organization of meetings of employee representative bodies.

- Legal obligation

Remuneration management

and accomplishment

administrative formalities

Establishment of remuneration, provision of pay slips

- Execution of the contract

Nominative social declaration.

- Legal obligation

Provision of IT tools to staff

Monitoring and maintenance of computer equipment.

- Legitimate interest

Management of IT directories to define access authorizations to applications and networks.

- Legitimate interest

Implementation of devices intended to ensure the security and proper functioning of computer applications and networks.

- Legitimate interest

Professional email management.

- Legitimate interest

Virtual private networks internal to the organization allowing the dissemination or collection of personnel administrative management data (intranet).

- Legitimate interest

Work organization

Management of diaries and professional projects.

- Legitimate interest

Career Tracking

and mobility

Professional evaluation of staff, in compliance with the legislative, regulatory or contractual provisions that govern it.

- Legitimate interest

Management of internal professional skills.

- Legitimate interest

Forward-looking employment and skills management (GPEC)

- Legitimate interest

Management of professional mobility.

- Execution of the contract

Training

Management of training requests and completed training periods.

- Execution of the contract

Organization of training sessions and evaluation of knowledge and training.

- Legitimate interest

Social assistance management

Management of social and cultural action directly implemented by the employer, excluding occupational medicine, social service or psychological support activities.

- Legitimate interest5. Personal data concerned

In order to minimize the personal data processed, the organization must ensure that it only collects and uses data that is

relevant and strictly necessary for its own personnel management needs. This may be data relating to:

a) The identification of the employee;

b) The assessment of the candidate's skills at the time of recruitment;

c) Career monitoring and employee training;

d) The establishment of the payslip and the related legal obligations (in particular, in the context of the deduction at source, the tax rate);

e) Validation of acquired experience;

f) To the management of the declarations of industrial accident and occupational disease, to the management of work stoppages and other cases of authorized absences and to the follow-up of the medical examinations of the employee;

g) Subjections or particular situations giving rise to the right to special leave or to a credit of hours of delegation;

h) The professional tools and materials made available to the employee as part of their assignments (i.e. payment cards, provision of computer equipment, etc.);

i) The management of social and cultural activities implemented by the employer;

j) Professional elections and meetings of employee representative bodies;

k) The fight against discrimination, the employment obligation resulting from articles L. 5212-2 and following of the labor code, etc.

In general, the employer should only collect the data he really needs, and should only do so when this need materializes.

Example 1: when concluding an employment contract, the employer has the obligation to carry out certain declarative formalities which require the processing of the social security number (NIR) of the employees. If this use is then justified, it cannot be requested from a candidate before the final validation of his application.

Example 2: the information that may be requested from a candidate for employment must have a direct link with the assessment of his professional qualities and skills, and must therefore not relate to the composition of his family, to information relating to relatives, etc. On the other hand, when an employee in post requests to benefit from a specific leave for the death or the accompaniment of serious illness of a relative, the employer can require the production of documents establishing the reality of the situations invoked. Data, the processing of which is justified for a specific purpose, may only be reused for other purposes if this use is itself legally justified.

In addition, certain categories of data call for increased vigilance due to their particularly sensitive nature. Benefiting from special protection, they can only be collected and processed under conditions strictly defined by the texts.

These include:- the social security number;

- data relating to offences, criminal convictions and related security measures.

Example: following an accident at work involving one of his employees, the employer completes an accident report in which he must indicate the nature and location of the victim's injuries. However, these data relate to the employee's state of health and therefore constitute sensitive data. Their processing is therefore in principle prohibited under Article 9.1 of the GDPR. However, the employer benefits from an exception to process them on the basis of Article 9-2-b) of the GDPR (the processing is necessary for the purposes of the performance of the obligations and the exercise of the rights specific to the responsible for the processing or to the person concerned with regard to labor law, social security and social protection […]).

In certain very limited cases:- sensitive data (article 9 of the GDPR, articles 6 and 44 of the LIL), i.e. those which reveal ethnic or allegedly racial origin, political opinions, religious beliefs or philosophical or union membership of a person, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation.

A table reproduced below lists the data that can be collected and processed according to the purposes of the processing.

Data categories

Sample Data

Employee ID

Data relating to identity: surname, first name, photograph (optional), sex, date and place of birth, nationality, professional details, personal details (optional), passport references (only for staff required to travel to the foreign), family situation, marital status, dependent children, type of driver's license held by the employee.

Data relating to the professional situation: place of work, internal identification number, date of entry into the company, seniority, job held and hierarchical coefficient, accounting section, nature of the employment contract, degree of invalidity, recognition of the status of disabled worker (RQTH), other categories of beneficiaries of law no. 87-517 of July 10, 1987 (disabled pensioner, war disabled, assimilated war disabled).

Data relating to the title equivalent to a work permit: type, serial number and copy of the title for foreign employees pursuant to article R. 620-3 of the labor code.

Contact details of people to notify in case of emergency.

Honors.

Career Tracking

and training

of the employee

Management of the employee's career: date and conditions of recruitment, date, subject and reason for changes made to the employee's professional situation, career simulation, employee wishes in terms of employment, disciplinary sanctions against the exclusion of those consecutive to acts amnestied.

Professional evaluation of the employee: dates of the evaluation interviews, identity of the evaluator, professional skills of the employee, objectives assigned, results obtained, assessment of professional skills on the basis of objective criteria and presenting a direct and necessary link with the job held, observations and wishes expressed by the employee, career development forecasts.

Training: diplomas, certificates and attestations, foreign languages spoken, follow-up of professional training requests and training periods carried out, organization of training sessions, evaluation of knowledge and training.

Administrative follow-up of the medical visits of employees: dates of the visits, aptitude for the work station (fit or unfit, proposals for adaptation of the work station or assignment to another work station formulated by the occupational doctor).

Establishment of payslips

and related legal obligations

Social security number under the conditions set by decree no. 2019-341 of April 19, 2019 or by article L. 444-5 of the labor code, numbers assigned by social insurance, retirement and provident organizations , family situation, marital status, dependent children, system and basis for calculating remuneration, elements determining the allocation of additional remuneration, leave and absences giving rise to deductible or compensable deductions, as well as any deduction legally operated by the employer, professional expenses, withholding tax rate, data transmitted via the Nominative Social Declaration.

Validation of achievements

experience

Date of the validation request, diploma, title or certificate of qualification concerned, professional experience subject to

validation, validation (yes/no), date of the decision.

Management of declarations of accidents at work and illness,

other absences

Contact details of the occupational physician, date of the accident or of the first medical observation of the illness, date of the last day of work, date of resumption, reason for the stop (work accident or occupational disease), work not resumed at date and other elements necessary for the said declarations.

Specific constraints giving right to special leave or to a credit of hours of delegation

Data relating to the exercise of an elected or representative union mandate, participation in the operational reserve or volunteer firefighter missions.

Tools and equipment made available to the employee as part of his professional duties

Internal directories and organization charts: surname, first name, photograph (optional), function, professional contact details, if applicable, training and professional achievements.

Professional diaries: dates, places and times of professional appointments, subject, people present.

Staff tasks: identification of the staff concerned, distribution of tasks.

Management of individual allocations of supplies, equipment, vehicles and payment cards: management of requests, nature of the allocation, dates of allocation, maintenance and withdrawal, budget allocations.

Computer directories for defining access permissions to applications and networks.

Connection data recorded to ensure the security and proper functioning of applications and computer networks, excluding any processing allowing individual control of the activity of employees.

Electronic messaging: address book, individual accounts, excluding any data relating to the individual control of electronic communications sent or received by employees.

Virtual private networks for the dissemination or collection of personnel administrative management data (intranet): internal administrative forms, organizational charts, discussion areas, information areas.

Social activities and implemented by the employer

Identity of the employee and his dependents or eligible persons, income, advantages and benefits requested and paid.

Relations with employee representative bodies

Summonses, preparatory documents, minutes, miscellaneous minutes.

After ensuring the necessity and relevance of the personal data it processes, the organization must also ensure, throughout the lifetime of the processing, the quality of this data which must be accurate and up-to-date.

6. Recipients of the data Personal data must only be made accessible to persons authorized to know it with regard to their attributions.

Access authorizations must be documented by the organisations, and access to the various processing operations must be subject to traceability measures (see point relating to security).

The data controller who wishes to use a subcontractor must ensure that he only uses organizations that offer sufficient guarantees. A contract defining the characteristics of the processing as well as the different obligations of the parties in terms of data protection must be established between them (article 28 of the GDPR). A subcontractor's guide, published by the CNIL, specifies these obligations and the clauses to be included in the contracts.

6.1. Persons accessing data on behalf of the employerOnly persons authorized by virtue of their missions or functions must be able to access the personal data processed, and this, within the strict limits of their respective attributions and of the accomplishment of these missions and functions. They may be, for example: - authorized persons in charge of personnel management or payroll management;

- authorized persons responsible for ensuring the safety of people and property, for the purposes of controlling access to premises and work tools;

- the hierarchical superiors of the employees concerned, excluding data relating to the social action directly implemented by the employer.

6.2. Recipients of dataThe GDPR defines recipients as any organization that receives the communication of data.

In the context of this repository, the following may in particular be recipients of the data:

- the staff representative bodies, for the data strictly necessary for their missions under the conditions set by the applicable texts;

- the bodies managing the various social insurance, unemployment insurance, retirement and welfare systems, the paid leave funds, the public bodies and administrations legally authorized to receive them;

- the entities responsible for the audit and financial control of the employing organization;

- the various service providers to whom the employing organization is likely to subcontract the management of certain activities (collective catering, electronic voting, archiving of documents, maintenance of savings accounts, etc.);

- entities in charge of cultural and social action such as social and economic committees (CSE), provided that the beneficiary has requested it.

To ensure the continuity of the protection of personal data, their transfer outside the European Union is subject to specific rules. Thus, in accordance with the provisions of Articles 44 et seq. of the GDPR, any transmission of data outside the EU must:- be based on an adequacy decision;

- or be governed by internal corporate rules (BCR), standard data protection clauses, a code of conduct or a certification mechanism approved by the CNIL;

- or be framed by ad hoc contractual clauses previously authorized by the CNIL;

- or respond to one of the derogations provided for in Article 49 of the GDPR. To find out more, consult the section Transferring data outside the EU on the CNIL website.

7. Storage periods In accordance with Article 5-1-e of the GDPR, personal data must only be kept in a form allowing the identification of persons for the time strictly necessary for the achievement of the purposes pursued. It is therefore with regard to the purpose that the retention period will be determined.

The data retention period or, when it is impossible to fix it, the criteria used to determine this period, is part of the information that must be communicated to the persons concerned.

Under these conditions, it is the responsibility of the controller to determine this duration before the processing is carried out.

For example, many data necessary for the management of the contractual relationship (employment contract) must be kept for the duration of the employment relationship, unless otherwise provided by law or regulation.

However, this does not preclude their conservation in the form of intermediate archives separate from the active database, with restricted access, insofar as there are specific legislative or regulatory provisions (for example, to meet accounting, social or tax, or if these data would be of interest in the event of litigation, justifying their retention for the time of the applicable prescription/foreclosure rules.

To find out more, you can refer to the CNIL guides:- Security: Secure archiving;

- Limit data retention.

Data used for statistical purposes are no longer qualified as personal data once they have been duly anonymised (see EDPS guidelines on anonymisation). The following table contains practical illustrations of retention periods that may, depending on the context, be retained by the organizations concerned:

Processing activities

Processing details

active base

Intermediate archiving

Reference texts

Payroll management

payslip

1 month

5 years

L. 3243-4 of the labor code

50 years in dematerialized version

D. 3243-8 of the labor code

Elements necessary for the calculation of the tax base

1 month

6 years

L. 243-16 of the social security code

Entering calculated data (DSN)

The time required to complete the declaration

6 years

L. 243-16 of the social security code

Transfer order for payment

The time required to issue the payslip

10 years from the end of the financial year

L. 123-22 of the Commercial Code

Single staff register

The length of time the employee is on the staff

5 years from the departure of the employee from the organization

R. 1221-26 of the labor code

Management of mandates of staff representatives

Nature of mandate and membership union

6 months after the end of the mandate

6 years (penal prescription for misdemeanor)

L. 2411-5 of the labor code

Management of mandates of staff representatives

Data relating to specific constraints giving rise to the right to special leave or credit for hours of delegation (e.g. exercise of an elective or union representative mandate)

The time of the hardship period of the employee concerned

6 years (penal prescription for misdemeanor)

L. 2142-1-3 of the labor code

8. Information of personsIt is the responsibility of the data controller to ensure compliance with the principles of transparency and fairness with regard to the persons whose data may be processed under the conditions provided for in Articles 12, 13 and 14 of the GDPR.

Thus, from the stage of the collection of personal data, the persons concerned must be informed of the existence of the processing, of its characteristics and of the rights available to them under the applicable regulations on the protection of personal data.

Information models are available on the CNIL website and can be consulted in the GDPR section: examples of information notices.

If the GDPR does not impose any specific form, written information must be privileged so as to be able to justify its content, as well as the time when it was issued.

Furthermore, in the context of an employment relationship, the data controller must also ensure that he complies with his other transparency obligations arising from the social legislation to which he is subject.

The labor code thus requires employers to inform their employees individually in certain situations.

Similarly, it is up to data controllers to ensure, with regard to the regulations applicable to them, compliance with any obligation to inform and/or consult the competent employee representative bodies.

9. Rights of persons The persons concerned have the following rights, which they exercise under the conditions provided for by the GDPR (see the section entitled Understanding my rights on the CNIL website): - the right to oppose the processing of their data, provided that it is provided for in application of the provisions of Article 21 of the GDPR.

With regard to personnel management processing: - the right of opposition does not exist when the processing meets a legal obligation, if it is necessary for the performance of a contract or is, exceptionally, based on the consent of the employee (to the extent that, in the latter case, the person concerned may withdraw consent to the processing of their data);

- on the other hand, the right of opposition may be exercised, provided that the person invokes reasons relating to his particular situation, when the processing is implemented on the basis of the legitimate interest of the data controller, or for the performance of a task in the public interest or a task relating to the exercise of public authority;

- the right to access, rectify and, under specific conditions, erase data concerning them;

- the right to limit processing (for example, when the person disputes the accuracy of their data, they can ask the organization to temporarily freeze the processing of their data, while the latter carries out checks required) ;

- the right to portability: the organization must allow any person to receive, in a structured and commonly used format, all the data processed by automated means. The data subject may request that his data be transmitted directly by the initial body to another body. Only data provided by the data subject on the basis of his consent or a contract are concerned. It is therefore recommended to specify to the persons the processing concerned by this right to portability.

10. SecurityThe organization must take all necessary precautions with regard to the risks presented by its processing to preserve the security of personal data and, in particular at the time of their collection, during their transmission and their storage, to prevent them from being distorted. , damaged or that unauthorized third parties have access to it.

In particular, in the specific context of this standard, either the organization adopts the following measures, or it justifies their equivalence or the fact of not needing or being able to use them:

Categories

Measures

Educate users

Inform and raise awareness of the people handling the data

Write an IT charter and give it binding force

Authenticate users

Define a unique identifier (login) for each user

Adopt a user password policy in accordance with the recommendations of the CNIL

Force user to change password after reset

Limit the number of attempts to access an account

Manage authorizations

Define authorization profiles

Remove obsolete access permissions

Carry out an annual review of authorizations

Trace access and manage incidents

Provide a logging system

Inform users of the implementation of the logging system

Protect logging equipment and logged information

Provide procedures for personal data breach notifications

Securing workstations

Provide an automatic session locking procedure

Use regularly updated anti-virus software

Install a software firewall

Obtain the user's agreement before any intervention on his workstation

Securing Mobile Computing

Provide encryption means for mobile equipment

Make regular data backups or synchronizations

Require a secret for unlocking smartphones

Protect the internal computer network

Limit network flows to what is strictly necessary

Securing the remote access of mobile computing devices by VPN

Implement WPA2 or WPA2-PSK protocol for Wi-Fi networks

Securing servers

Limit access to administration tools and interfaces to authorized persons only

Install critical updates without delay

Ensure data availability

Securing websites

Use the TLS protocol and verify its implementation

Check that no password or identifier passes through the urls

Check that user input matches what is expected

Put a consent banner for cookies not necessary for the service

Back up and plan for business continuity

Perform regular backups

Store backup media in a safe place

Provide security means for the transport of backups

Plan and regularly test business continuity

Archive securely

Implement specific access procedures for archived data

Securely destroy obsolete archives

Supervise the maintenance and destruction of data

Record maintenance interventions in a logbook

Supervise by a person in charge of the organization the interventions by third parties

Erase data from any hardware before disposal

Manage subcontracting

Relations with service providers who process data in the name and on behalf of the data controller (the employing body) must be the subject of a written agreement.

This agreement must contain one or more specific clauses relating to the respective obligations of the parties resulting from the processing of personal data.

The agreement must in particular provide for the conditions for the restitution and destruction of the data. It is the responsibility of the data controller to ensure the effectiveness of the guarantees provided (security audits, visits, etc.).

For more details, you can refer to the subcontracting guide and the examples of subcontracting clauses.

Secure exchanges with other organizations

Encrypt data before sending

Make sure it's the right recipient

Transmit the secret in a separate send and through a different channel

Protect the premises

Restrict access to premises with locked doors

Install intruder alarms and check them periodically

Supervise IT developments

Offer privacy-friendly settings to end users

Strictly regulate free comment areas

Test on fictitious or anonymized data

Use cryptographic functions

Use recognized algorithms, software and libraries

Keep secrets and cryptographic keys securely To do this, the data controller can usefully refer to the Personal Data Security Guide.

11. Impact analysis relating to data protection (DPIA) Pursuant to the provisions of Article 35 of the GDPR, the controller may have to carry out an impact analysis when the processing it implements work is likely to pose a high risk to the rights and

freedoms of data subjects.

First of all, you should refer to:- the list of processing operations for which an impact analysis is not required;

Types of processing operations

Examples

Processing, implemented solely for human resources purposes and under the conditions provided for by the applicable texts, for the sole management of the personnel of organizations that employ less than 250 people, with the exception of the use of profiling.

Treatments allowing:

- payroll management, issue of payslips;

- training management;

- the management of the company restaurant, the delivery of meal vouchers;

- reimbursement of professional expenses;

- the follow-up of the annual appraisal interviews;

the keeping of the obligatory registers;

- the use of communication tools (electronic messaging, telephony, videoconferencing, online collaborative tools) without recourse to profiling or biometrics;

- control of working time (without biometric device, without sensitive or highly personal data);

Processing implemented for the sole purpose of managing physical access controls, apart from any biometric device.

Excluding data processing that reveals sensitive or highly personal data.

Processing for the purpose of:

- the implementation of a device by badge without biometrics to enter the premises of an organization for security purposes;

- the implementation of a system for monitoring the working time carried out by employees, to the exclusion of any other purpose; - then, to the list of types of processing operations for which a relative impact analysis data protection is required.

Types of processing operations

Examples

Processing operations establishing profiles of natural persons for human resources management purposes

Processing for the purpose of:

- processing aimed at facilitating recruitment, in particular through a selection algorithm;

- processing aimed at offering personalized training actions using an algorithm;

- processing aimed at detecting and preventing the departure of employees on the basis of correlations established between various factors;

Processing for the purpose of constantly monitoring the activity of the employees concerned

Processing for the purpose of:

- analysis of outgoing e-mail flows in order to detect possible information leaks (so-called Data Loss Prevention systems);

- video surveillance of employees handling cash;

- video surveillance of a warehouse storing valuable goods in which handlers work;

- the tachograph function of road transport vehicles. - if the processing implemented is not present on one of these lists, it is then necessary to question the need to carry out a DPIA.

This should be done using the criteria established by the European Data Protection Board (EDPB) in the Guidelines for Data Protection Impact Assessment (DPIA).

In accordance with this text, carrying out a DPIA is mandatory when at least two of the nine criteria are met: - assessment or rating of a person;

- automated decision-making;

- systematic monitoring;

- processing of sensitive or highly personal data;

- large-scale treatment;

- crossing or combination of data sets;

- data concerning vulnerable persons;

- innovative use or application of new technological or organizational solutions;

- processing that prevents people from exercising a right or benefiting from a service or a contract.

Please note: the EDPS Guidelines clarify that employees may be considered vulnerable data subjects due to the heightened power imbalance that exists between them and the controller (the employer).

To carry out an impact study, the data controller may refer to:- the principles contained in this reference system;

- the methodological tools offered by the CNIL on its website.

If the organization has designated one, the DPO must be consulted.

In accordance with Article 36 of the GDPR, the data controller must consult the CNIL prior to the implementation of the processing if the impact analysis indicates that he is unable to identify sufficient measures to reduce the risks to a acceptable level.

The president,

M. L. Denis