Deliberation 2019-139 of July 18, 2019 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Wednesday December 11, 2019 NOR: CNIL1935146X of personal data intended for the implementation of a whistleblowing systemThe National Commission for Data Processing 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 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free circulation of this data; Having regard to the Commercial Code, in particular its Articles L. 225-102-3 and R. 822-33; Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, data yesterdays and freedoms; Having regard to law n° 2016-1691 of December 9, 2016 relating to transparency, the fight against corruption and the modernization of economic life (Sapin law 2), in particular its articles 6, 8 and 17 ;Having regard to Law No. 2017-399 of March 27, 2017 relating to the duty of vigilance of parent companies and ordering companies (Duty of Vigilance Law);Having regard to Decree No. 2017-564 of April 19, 2017 relating to procedures collection of reports issued by whistleblowers within legal entities governed by public or private law or State administrations; Having regard to decree no. Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to the recommendations of the French Anti-Corruption Agency intended to help legal persons governed by public and private law to prevent and detect the facts of corruption, influence peddling, misappropriation, illegal taking interest, embezzlement of public funds and favouritism; 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 intended for the implementation of a professional alert system, which will be published in the Official Journal of the French Republic.ANNEX1. Who is this reference for?

This standard is intended for private or public organizations which are required or which decide to implement a system for collecting and managing professional alerts requiring the processing of personal data. It therefore covers two types of devices.

On the one hand, this standard concerns alert systems governed by specific legislative or regulatory provisions, whether or not the organization is legally subject to these provisions. This may include, in particular, the systems provided for in Articles 8 and/or 17 of the so-called Sapin 2 law (1), or implemented pursuant to the law relating to the duty of vigilance (2), whatever regardless of the size of the workforce, the legal nature or even the turnover of the organizations concerned.

In this first hypothesis, constitutes a professional alert any report made in good faith and which reveals or signals a criminal

offence, a serious and manifest violation of an international commitment duly ratified or approved by France, of a unilateral act of a international organization taken on the basis of such a commitment, law or regulation, or a serious threat or harm to the general interest, when the facts in question are not covered by national defense secrecy, the medical secrecy or the secrecy of relations between a lawyer and his client.

On the other hand, this standard is also intended to govern the ethical alert systems adopted on its own initiative by an organization with a view to prohibiting behavior deemed incompatible with its ethical charter or its internal regulations.

In this second hypothesis, constitutes a whistleblowing any report made in good faith and which reveals or signals a violation of the ethical rules adopted by an organization or a group, when the rules in question are codified in a written document (such as rules of procedure, an ethical charter, etc.) which respects the entire existing legal framework (in particular labor legislation and all the rights and fundamental freedoms of the persons concerned), and whose existence and enforceability are brought to the attention of all the persons concerned beforehand.

Organizations setting up a whistleblowing system must ensure its compliance:

- the provisions of the General Data Protection Regulations (GDPR) as well as those of the law of January 6, 1978 known as data processing and freedoms (LIL). Indeed, when these devices, as is the case as a general rule, require the processing of data relating to identified or identifiable natural persons (in particular those of the author and the person or persons targeted by the alert), they are subject to the rules relating to the protection of personal data;
- to all other rules of law applicable under specific legislation (the so-called Sapin 2 law, etc.) or general legislation (labour law).

The data controller must guarantee respect for the rights and fundamental freedoms as well as the legitimate interests of the persons concerned.

In the absence of a precise framework by the legislative and regulatory texts in force, the mechanisms created on the initiative of the organizations in the form, for example, of ethical charters or in their internal regulations must be the subject of particular attention.

2. Scope of the standard

The purpose of this repository is to provide a tool to help public and private organizations wishing to set up systems for processing professional alerts comply with the regulations relating to the protection of private data.

Compliance with this standard enables organizations to ensure compliance of the data processing implemented within the

framework of the alert systems 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 system also constitutes an aid to carrying out an impact analysis relating to data protection (DPIA).

The establishment of a whistleblowing system must in fact systematically give rise to the prior completion of a DPIA. Indeed, these devices appear in the list of types of processing operations for which an impact analysis relating to data protection is required (see deliberation no. 2018-327 of October 11, 2018 adopting the list types of processing operations for which a data protection impact assessment is required).

To carry out an impact study, the data controller may refer to the methodological tools offered by the CNIL on its website. It may also refer to this reference system for 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 the control of their risks (point 10). To this end, the organization may refer to the CNIL guidelines on data protection impact assessments (AIPD).

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 organization.

With regard to the alert system, data processing is implemented in order to collect and process alerts or reports aimed at revealing a breach of a specific rule.

Example 1.1 (alerts from Article 8 of the Sapin 2 Law):

An alert system implemented to meet the requirements of Article 8.III of the Sapin 2 law aims to allow staff members and external and occasional collaborators of an organization to report:

- a crime or offence;

- a serious and manifest violation of an international commitment duly ratified or approved by France;

- a serious and manifest violation of a unilateral act of an international organization taken on the basis of a duly ratified international commitment;

- a serious and manifest violation of the law or regulation;

- a serious threat or harm to the general interest, of which the issuer of the alert has personal knowledge.

Example 1.2 (fight against corruption and influence peddling):

A whistleblowing system implemented to meet the requirements of Article 17.II.2° of the Sapin 2 law aims to collect reports from employees of the organization concerned and relating to the existence of conduct or situations contrary to the company's code of conduct and likely to characterize acts of corruption or influence peddling.

Example 1.3 (duty of care):

An alert system provided for in Article L. 225-102-4 of the Commercial Code, resulting from the so-called Duty of Vigilance Law, will be intended to collect reports relating to the existence or realization of risks. serious violations of human rights and fundamental freedoms, the health and safety of people and the environment, resulting from the activities of the company and those of the companies it controls within the meaning of II of article L 233-16, directly or indirectly, as well as the activities of subcontractors or suppliers with whom an established commercial relationship is maintained, when these activities are attached to this relationship.

Example 2 (ethical codes):

An alert system put in place on a voluntary basis by the body, apart from a specific legal obligation, could for example have the purpose of collecting any report of an existing or realized risk of behavior or behavior. a situation contrary to an ethical charter of the organization, regardless of the author of the alert or his link with the organization.

Example 3 (hybrid devices):

A system targeting both common law alerts (article 8.III of the Sapin 2 law), those responding to the duty of vigilance (art. L. 225-102-4 of the commercial code) and those resulting from application of a charter or code of ethics, must explicitly target all the corresponding purposes, distinguishing those resulting from a specific mandatory provision from those voluntarily adopted by the organization.

The information collected for one of these purposes cannot be reused to pursue another objective that would be incompatible with the primary 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 processing

Each purpose of the processing must be based on one of the legal bases set by the regulations. The different bases authorizing an organization to process personal data as part of a whistleblowing system are listed below.

In the context of this processing, the legal basis may be:

a) Compliance with a legal obligation incumbent on the body, requiring the implementation of a whistleblowing system;

In order to be able to invoke this basis, the controller ensures that the following conditions are met:

- the obligation to implement a whistleblowing system results from an internal source of French law (for example, the Sapin law and its implementing decree), from an international commitment signed and ratified by France (by example, an international convention), or even the law derived from international and European organizations of which France is a party;
- the organization is actually subject to it with regard to the criteria retained by the regulations in question (for example, exceeding the thresholds for the size of the workforce, the turnover, the carrying out of operations of a certain nature, etc.) .

b) The fulfillment 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.

This legal basis applies when the establishment of an alert system does not result from a legal obligation imposed on the controller.

It is the responsibility of each data controller to ensure the choice of one and/or the other of these bases, depending on the rules applicable to his entity.

When a device meets a specific legal obligation (for example, those resulting from Articles 8 and/or 17 of the Sapin II Law, the Duty of Vigilance Law, etc.), while allowing the collection of alerts relating to a voluntary commitment by the organization (for example, provided for by an internal code of ethics, or even provided for by a legislative text to which the organization is not legally subject), it is up to the data controller to distinguish the legal bases on which each of these purposes.

5. Personal data concerned

5.1. Principles of relevance and data minimization

5.1.1. At the alert stage

In general, the data controller must ensure that only the data necessary for the pursuit of the purposes of the processing are actually collected and processed. In this respect, particular attention must be paid to facts that may be reported via professional whistleblowing systems set up, on their own initiative, by organizations that are not subject to specific obligations in this regard. In the absence of a specific framework by the legislative and regulatory texts in force, it is the responsibility of the controller to ensure in particular that, in this case, the rights, freedoms and legitimate interests of all persons who may be affected by an alert.

However, in the case of whistleblowing systems, only the whistleblower is able to determine the nature and volume of information, particularly of a personal nature, communicated during the report.

Therefore, the data controller must remind the authors of reports that the information communicated in the context of an alert system must remain factual and present a direct link with the subject of the alert.

5.1.2. At the alert investigation stage

For the purposes of this reference system, the instruction phase of an alert is understood as the period which begins with the reception of the alert by the organization, and which ends with the decision being taken as to the follow-up reserved for that -this.

This phase allows the organization to conduct an investigation into the facts reported. During this period, the whistleblowing system can be used to document the steps taken by the organization in this regard (legal and technical analysis of the facts, collection of evidence, exchanges with various stakeholders, hearing of witnesses, carrying out acts of expertise, etc.).

The instruction phase is characterized by the role of the data controller in determining the elements that may be collected or stored in the system.

It is therefore up to him to ensure that only the information that is relevant and necessary with regard to the purposes of the processing is collected and/or stored in the alert system. This is generally the case for the following categories:

- identity, functions and contact details of the issuer of the alert;
- identity, functions and contact details of the persons subject to the alert;
- identity, functions and contact details of the persons involved in collecting or processing the alert;
- reported facts;
- elements collected as part of the verification of the facts reported;

- reports of verification operations;

- follow-up given to the alert.

5.2. The processing of sensitive data and infringement data

Two categories of data call for heightened vigilance.

On the one hand, certain data, due to their particularly sensitive nature, in particular those which reveal the ethnic or allegedly racial origin, political opinions, religious or philosophical beliefs or trade union membership of a person, genetic data , biometric data, data concerning health or data concerning a person's sex life or sexual orientation enjoy special protection and may only be processed subject to compliance with specific conditions set out in Article 9 GDPR and Articles 6 and 44 LIL.

In the context of this processing, these data may in particular be processed when the processing is necessary for the establishment, exercise or defense of a legal right, in accordance with Article 9-2-f of the GDPR.

On the other hand, the data collected and processed within the framework of the systems for collecting professional alerts may also include data relating to offences, convictions and security measures concerning natural persons. Such data can only be collected and processed under the conditions strictly defined in Article 10 of the GDPR and Article 46 of the LIL.

In the context of this processing, the collection of this data may be authorized:

- by specific provisions of national law (for example, articles 8 or 17 of the Sapin 2 Law, article L. 225-102-4.-I. of the Commercial Code, etc.);

- or to allow the data controller to prepare and, where appropriate, to exercise and monitor legal action as a victim, accused, or on behalf of them, in accordance with Article 46 -3° LIL.

5.4. Processing the identity of the author of an alert

An alert device can require or propose that the author of the alert identifies himself.

If the issuer of the professional alert must identify himself, his identity is treated confidentially by the organization or the persons responsible for managing the alerts.

However, it is recommended that the organization does not encourage people intended to use the system to do so anonymously, it being understood that an anonymous alert is an alert whose author is neither identified nor identifiable.

As an exception, the alert of a person who wishes to remain anonymous should be processed under the following conditions:

- the seriousness of the facts mentioned is established and the factual elements are sufficiently detailed;

- the processing of this alert must be surrounded by special precautions, such as a prior examination, by its first recipient, of the advisability of its dissemination within the framework of the system.

After ensuring the necessity and relevance of the personal data it uses, the organization must also ensure, throughout the lifetime of the processing, the quality of the data it processes. . In practice, this means that in accordance with the regulations, the data is accurate and up-to-date.

6. Recipients of information

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 organizations, and access to the various processing operations must be subject to traceability measures. See point 9 relating to safety.

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 employer

Only persons authorized by virtue of their missions or functions should be able to access the personal data processed, and this within the strict limits of their respective attributions and the accomplishment of these missions and functions.

It can be, for example:

- persons specifically responsible for managing alerts within the organisation;

- the referent or service provider responsible for collecting and processing alerts. The referent or service provider possibly appointed to manage all or part of this system undertakes in particular, by contractual means, not to use the data for purposes other than the management of alerts, to ensure their confidentiality, to respect the duration limited storage of data and to proceed with the destruction or return of all manual or computerized personal data media at the end of its service.

6.2. Data recipients

The GDPR defines recipients as any organization that receives the data communication.

As part of this processing, the data may be communicated within the group of companies to which the organization concerned belongs if this communication is necessary solely for the purposes of checking or processing the alert.

Certain legal or regulatory provisions strictly regulate the communication of information. Thus, the elements likely to identify the issuer of the alert can only be disclosed, except to the judicial authority, with the consent of the person. Similarly, elements likely to identify the person implicated by a report may only be disclosed, except to the judicial authority, once the justified nature of the alert has been established.

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 and following 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 meet one of the derogations provided for in Article 49 of the GDPR.

To find out more, see 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 this is not possible, 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.

7.1. Storage periods

With regard to the purposes that may justify the establishment of a whistleblowing system, and unless otherwise provided by law or regulation:

- the data relating to an alert considered by the controller as not falling within the scope of the system, are immediately destroyed from the professional alert system or anonymized in accordance with Opinion 05/2014 relating to anonymization techniques of the European Data Protection Board (EDPB).

- When no follow-up is given to an alert falling within the scope of the system, the data relating to this alert is destroyed or anonymized by the organization responsible for managing the alerts, within a period of two months from the closure of verification operations. For the purposes of this standard, the expression follow-up designates any decision taken by the organization to draw conclusions from the alert. This may involve the adoption or modification of the internal rules (internal regulations, ethical charter, etc.) of the organization, a reorganization of the operations or services of the company, the pronouncement of a sanction or the implementation of legal action.

The Commission recalls that decisions relating to the action taken on professional alerts must be taken within a reasonable period of time from their issuance.

- When a disciplinary or litigation procedure is initiated against a person in question or the author of an abusive alert, the data relating to the alert may be kept by the organization responsible for managing alerts until the end of the procedure or the prescription of appeals against the decision.

With the exception of cases where no follow-up is given to the alert, the data controller may keep the data collected in the form of intermediate archives for the purposes of ensuring the protection of the whistleblower or of allowing the findings of continuing violations. This retention period must be strictly limited to the purposes pursued, determined in advance and brought to the attention of the persons concerned.

The data may be kept longer, in intermediate archiving, if the controller has a legal obligation (for example, to meet accounting, social or tax obligations).

7.2. Retention of anonymized data

The regulations relating to the protection of personal data do not apply, in particular with regard to retention periods, to anonymous data, i.e. data which can no longer be linked to one or identified or identifiable natural persons.

Therefore, the data controller may keep the anonymized data indefinitely. In this case, the organization concerned must guarantee the anonymized nature of the data in a sustainable manner.

To find out more, you can refer to the CNIL guides:

- Security: Archive securely;

- 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).

Example :

An organization is subject to the obligation to set up an alert system in application of the provisions of article 8 of the Sapin 2 law (general alert system), but also an alert system in application of the Article 17-II-2° of the same law (system aimed at allowing the reporting of breaches or situations contrary to the organization's code of conduct, in the context of the fight against corruption and influence peddling).

It is then possible for the organization to set up a single tool for collecting these reports. However, there may be differences in the legislative and regulatory framework for processing. Thus, the procedures for setting up general alert systems are governed, in particular with regard to retention periods, by decree no. 2017-564 of April 19, 2017 relating to the procedures for collecting reports issued by launchers. alert within legal entities under public or private law or State administrations.

However, this decree is not applicable to the fight against corruption and influence peddling. The data collected via the specific alert systems are therefore not subject to any particular supervision and their processing must be supervised in application of the regulations.

The implementation of a single tool for collecting reports involves complying with the legislative and regulatory requirements of each of the systems, and in particular:

- differentiate the treatment applied to reports relating to suspicions or facts of corruption from that applied to other reports;
- to apply different retention periods depending on whether the data is collected within the framework of one or other of the alert systems.

8. Information of persons

It is the responsibility of the data controller who decides to set up a whistleblowing system to ensure compliance with the principles of transparency and fairness with regard to the persons whose data may be processed.

Compliance with this obligation presupposes informing the persons concerned individually and collectively, according to the methods described below.

8.1. Identification of data subjects

For the purposes of this reference system, all persons who can potentially issue a report via the system or be targeted by an alert are considered to be persons potentially concerned by a whistleblowing system, and in particular:

- The staff of the organization concerned, regardless of the legal status of the collaboration (employees, agents, temporary workers, trainees, employees seconded by a third party, volunteers, etc.);

- The collaborators, customers and external suppliers of the organization, when they are natural persons having a direct contractual link with the organization (consultants, agents, advisers, subcontractors natural persons with self-employed status, etc. .);

- The workforce (employees, partners, managers, etc.) of legal entities that have a contractual relationship with the organization concerned.

Persons concerned by a whistleblowing system are all persons whose personal data are actually processed within the framework of the system (for example, the authors of the alerts, the persons concerned, the persons heard within the framework of the investigation, etc.).

8.2. Content of the information to be delivered

The information communicated to the persons concerned must be provided under the conditions provided for in Articles 12, 13 and 14 of the GDPR.

In general, it must mention the existence of the processing, its characteristics (in particular the purposes pursued, the types of data likely to appear there, the types of people likely to issue the alert or to be the subject , the main stages of the procedure triggered by the alert, the data retention periods, etc.) as well as the rights available to the persons concerned.

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

8.3. Information methods

8.3.1. Consultations prior to setting up the system

It is the responsibility of data controllers to ensure, with regard to the regulations applicable to them, compliance with the obligation to inform and/or consult the competent authorities, when setting up alert systems. .

8.3.2. General information when deploying processing

In order to fully comply with the principles of fairness and transparency, the standard recommends that all persons potentially concerned by the system be informed prior to its introduction into the organization.

This information specifies the operation of the system, in particular the stages of the procedure for collecting reports, and in

particular the recipients and the conditions under which the alert can be sent to them.

The data controller expressly indicates that the misuse of the device may expose its author to sanctions or prosecution but that conversely, the use of the device in good faith will not expose its author to any disciplinary sanction, when well, even the facts would subsequently prove to be inaccurate or would give rise to no follow-up.

The data controller recalls that the whistleblowing system is only one means of reporting among others (as can the hierarchical channel), and that failure to use it cannot result in any sanction. against staff members.

The individual information of people (for example, by sending an e-mail to the person's personal mailbox, delivery of an individual information document in paper form, etc.) must be given priority as far as possible.

8.3.3. Whistleblower specific information

In accordance with Article 13 of the GDPR, persons who issue a report via the system must receive information relating to the processing from the start of the process of collecting the alert.

It can in particular take the form of a display of a page or a block of text, prior to the step of entering information relating to the alert. The data controller may make access subject to the performance of an action (for example, ticking a box) indicating that the author of the alert has taken note of this information.

When an alert is issued, an acknowledgment of receipt thereof must be provided to the whistleblower to enable the latter to benefit, where applicable, from a specific protection regime. This acknowledgment of receipt must be timestamped. It summarizes all the information and, where applicable, the attachments communicated as part of the report. The delivery of this receipt to the author of the alert must not be subject to the production of identifying information (e-mail or postal address, etc.) when the person wishes to remain anonymous.

When a decision on the follow-up to the alert has been taken by the data controller, the author of the alert is informed.

8.3.4. Specific information of the person targeted by the alert

In accordance with Article 14 of the GDPR, the data controller must inform the person concerned by an alert (for example, as a witness, victim or alleged perpetrator) within a reasonable period of time, which may not exceed one month, following the issuance of an alert.

Nevertheless, in accordance with Article 14-5-b of the GDPR, this information may be deferred when it is likely to seriously compromise the achievement of the objectives of the said processing. This could for example be the case when the disclosure

of this information to the person concerned would seriously compromise the requirements of the investigation, for example in the presence of a risk of destruction of evidence. The information must then be issued as soon as the risk has been eliminated.

This information is produced in accordance with methods that make it possible to ensure that it is properly delivered to the person concerned. It does not contain information relating to the identity of the issuer of the alert or that of third parties.

However, when a disciplinary sanction or a contentious procedure is initiated following the alert with regard to the person concerned, the latter may obtain the communication of these elements under the rules of common law (rights of defense in particular ).

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 respecting the rights of persons on the CNIL website):

- right to object to the processing of their data, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR;

- right of access, rectification and erasure of data concerning them;

- right to restriction of 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 the necessary checks.

9.1. Permission to access

Any person whose personal data is or has been the subject of processing in the context of a professional alert (whistleblower, presumed victims of the facts, persons targeted by the alert, witnesses and persons heard during the investigation, etc.), has the right to have access to it in accordance with the provisions of art. 15 GDPR.

The exercise of this right must not allow the person exercising it to access personal data relating to other natural persons.

This limitation is specific to the rules relating to the protection of personal data and does not preclude the application, where applicable, of the rules of procedural law, fundamental freedoms (and in particular the adversarial principle), etc.

9.2. Right of objection

In accordance with Article 21 of the GDPR, the right of opposition cannot be exercised for processing operations necessary for compliance with a legal obligation to which the controller is subject.

It cannot therefore be exercised with regard to processing implemented by companies fulfilling the conditions of Articles 8

and/or 17 of the Sapin II Law or those of Part I-4 of Article L. 225 -102-4 of the commercial code.

On the other hand, when an organization does not meet these conditions, but sets up an alert system on a purely voluntary basis, the right of opposition exists. Therefore, the persons concerned must be informed of its existence and the controller must ensure compliance with it.

However, the exercise of this right is not automatic: the person who exercises it must characterize the existence of reasons relating to his particular situation.

The data controller must take the opposition into account, unless it demonstrates:

- that there are legitimate and compelling reasons which prevail over the interests and the rights and interests of the person concerned or;
- that the processing is necessary for the establishment, exercise or defense of legal claims.

However, the facts likely to be the subject of a report are by their very nature linked to the recognition, exercise and defense of rights (in particular those of the victims or those responsible for the reported facts, or those of the organization, whether its civil or criminal liability may be incurred, or if the alert was not made in good faith but had the intention of harming the smooth running of the organization, etc.).

Under these conditions, it is up to the organizations concerned to examine each opposition request taking these criteria into account.

9.3. Right to rectification and erasure

The right of rectification, provided for in Article 16 of the GDPR, must be assessed with regard to the purpose of the processing.

In the case of whistleblowing systems, it must in particular not allow the retroactive modification of the elements contained in the alert or collected during its investigation. Its exercise, when admitted, must not lead to the impossibility of reconstructing the chronology of any changes to important elements of the investigation.

This right can therefore only be exercised to rectify factual data, the material accuracy of which can be verified by the controller on the basis of evidence, without the data being erased or replaced, even erroneous, initially collected.

The right to erasure is exercised under the conditions provided for in Article 17 of the GDPR.

10. Security

The 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, 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

Categories

Measures

Securing websites

Use the TLS protocol and verify its implementation

Check that no password or identifier is transmitted in 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

Include a specific clause in subcontractor contracts

Provide the conditions for restoring and destroying data

Ensure the effectiveness of the guarantees provided (security audits, visits, etc.)

Secure exchanges with other organizations

Encrypt data before it is sent

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

Test on fictitious or anonymized data

Use cryptographic functions

Use recognized algorithms, software and libraries

Store secrets and cryptographic keys securely

To do this, the data controller may usefully refer to the personal data security guide.

(1) Article 8 or Article 17-II-2° of Law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of economic life.

(2) Law no. 2017-399 of March 27, 2017 relating to the duty of vigilance of parent companies and ordering companies.

The president,

M. L. Denis