Deliberation 2021-131 of September 23, 2021 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Tuesday April 12, 2022 of personal data implemented for the purposes of managing commercial activitiesThe 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 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in particular its article 58 ;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8;

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

After having heard the report of Mr. François PELLEGRINI, Commissioner, and the observations of Mr. Benjamin TOUZANNE, Government Commissioner,

Adopts a standard relating to the processing of personal data implemented for the purposes of managing commercial activities.APPENDIXREFERENTIAL

RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED FOR THE PURPOSES OF MANAGING COMMERCIAL ACTIVITIES

You can consult the entire text with its images from the extract from the authenticated electronic Official Journal accessible at the bottom of page1. Who is this benchmark for? This benchmark offers ways to ensure compliance for "customer" and "prospect" files of private or public bodies.

Given the specific nature of their activities, this standard is not intended to provide a framework for the processing carried out by:

- health or educational establishments;

- banking or similar establishments;

- insurance companies;

- operators subject to the approval of the National Gaming Authority.2. Scope of the repository

The processing carried out in the context of the management of commercial activities, whether implemented using internal tools or outsourced to a service provider, leads to the collection of data relating to natural persons (customers, prospects). As such, they are subject to the provisions of 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 free movement. of these data (RGPD), the law of January 6, 1978 as amended, as well as the specific provisions relating to the protection of privacy in the electronic communications sector ("ePrivacy").

The bodies concerned, as data controllers, must put in place all the appropriate technical and organizational measures to guarantee a high level of protection of personal data from the design of the processing operations and throughout the life of the processing operations. this. They must also be able to demonstrate this compliance at any time. This processing must be recorded in the processing register, in accordance with the provisions of Article 30 of the GDPR (see the register models on the cnil.fr website).

The application of this reference system, which is not binding, makes it possible to ensure the compliance of processing for the management of commercial activities with the rules for the protection of personal data. Organizations can choose to deviate from the reference framework with regard to the specific conditions relating to their situation, making sure to take all the appropriate measures to guarantee their compliance with the GDPR.

This repository will be regularly updated by the CNIL in order to guarantee its compatibility with the latest legislative and technological developments.3. Objective(s) pursued by the processing (purposes)

The repository provides a framework for processing for the following purposes:

a) Contract management (for example: management of orders, delivery, performance of the service or supply of goods, invoices and payments);

b) Management of loyalty programs within one or more legal entities. In the latter case, the person must be, for example at the time of subscription to the loyalty program, explicitly informed, in particular, of the identity of the entity or entities considered as sole controller or jointly controllers and of the scope of the program and, if it involves the combination of personal data held by more than one entity;

c) Keeping the general accounts and the auxiliary accounts that may be attached to it;

d) Establishment of financial statistics concerning customers;

e) Follow-up of the customer relationship for the realization of satisfaction surveys, the management of complaints and after-sales service;

f) Selection of customers to carry out studies on the quality of products or consumer surveys (for example: product tests, sales statistics carried out by the organization concerned);

g) Carrying out commercial prospecting actions (for example: sending advertising messages, contests, sponsorship, promotion);

h) Management of people's opinions on products, services or content.

This processing may involve: - profiling carried out exclusively on the basis of data collected by the data controller directly from the data subject; Where

- updating contact data (telephone details, email addresses, physical addresses).

The information collected for one of these purposes cannot be reused to pursue another objective that would be incompatible with the purpose defined when it was collected. In addition, the processing implemented under this reference system must not give rise to interconnections or exchanges other than those necessary for the fulfillment of the purposes set out above.

Moreover, the reference system also provides indications relating to the operations transmission of data to third parties in order to enable them to carry out commercial prospecting operations by specifying the legal bases likely to be mobilized to found these operations (see point 6, below). Processing for the following purposes is not not affected by this standard:- detection and prevention of fraud;

- the temporary or permanent exclusion of persons from the benefit of a service or the supply of a good (for example, due to unpaid bills, customer incivility or abusive behavior);

- profiling carried out from data collected from sources third to the data controller, as well as those carried out from data collected through cookies and other tracers. On this point, see the guidelines relating to the application of article 82 of the law of January 6, 1978 as amended to read and write operations in a user's terminal (in particular to "cookies and other tracers") as well as as the recommendations proposing practical methods of compliance in the event of the use of "cookies and other tracers".4. Legal basis(s) of processing

Each purpose of the processing covered by the standard must be based on one of the legal bases set by the GDPR.a) The free, specific, informed and unambiguous consent of the data subject;

Consent requires, to be valid, a positive and specific action by the person concerned (eg: a dedicated checkbox that is not pre-ticked). As indicated by the EDPS, the acceptance of general conditions of use is not sufficient. The agreement must be free.

b) The execution, either of a contract to which the data subject is a party, or of pre-contractual measures taken at his request. The data collected must be necessary for the execution of contractual and/or pre-contractual measures. In this regard, the EDPS indicates that the fact that the contract concluded between the data subject and the controller mentions the collection of specific data is not sufficient to demonstrate that these data are necessary for the performance of the contract. Thus, to rely on this legal basis, the collection of data must be essential to provide the service or good expected by the data subject;

c) Compliance with a legal obligation incumbent on the organization;

d) The achievement of the legitimate interest pursued by the organization or by the third party, subject to not disregarding the interest or the fundamental rights and freedoms of the person concerned.

The table below, which is not intended to be exhaustive, lists examples of legal bases that can be used depending on each purpose pursued by the processing(s) covered by this reference system.

The legal bases must be brought to the attention of the persons whose data are processed since they make it possible, in particular, to determine their rights.

PRACTICAL ILLUSTRATION OF LEGAL BASES AND STORAGE PERIODS PURPOSE LEGAL BASIS RECOMMENDED STORAGE PERIOD Management of contracts / loyalty programs

Management of orders, delivery, execution of the service or supply of goods, etc.

Performance of the contract

Duration of the contractual relationship Bookkeeping

Accounting, tax obligations, etc.

Compliance with a legal obligation to retain data (for example, the obligation to ensure the identity of the person by requesting the provision of proof of identity)

In the form of an intermediate archive: legal retention period (for example, accounting obligation of 10 years). The identity document is kept for the time necessary to verify the identity of the person concerned. A copy of an identity document may be kept for a period of 6 years if it is necessary for the purposes of proof or to meet a legal obligation

customer relationship

Satisfaction surveys

Legitimate interest of the organization or Consent (*)

Duration necessary for the achievement of the purpose of the survey or until the exercise of the right of opposition or the withdrawal of consent

Claims management

Performance of the contract

Duration of the contractual relationship

After sales service

Performance of the contract

Duration of the contractual relationship Selection of clients / Studies / Surveys

Product quality studies

Legitimate interest of the organization or Consent (*)

Duration necessary for the achievement of the objective of the study or until the exercise of the right of opposition or the withdrawal of consent

Product testing

Sales statistics

Legitimate interest of the organization

Duration necessary for the achievement of the objective targeted by the statistics or until the exercise of the right of opposition

Commercial prospecting actions, (advertising messages, contests, sponsorship, promotion, etc.).

By electronic means (for the purpose of sending email, SMS, automated electronic communication system without human intervention, etc.), for goods or services that have not already been purchased by the persons concerned

Consent (see art. L. 34-5 of the CPCE)

Until consent is withdrawn or 3 years from the person's last contact with the organization

By post or automated call system giving rise to human intervention and telephone calls

Legitimate interest of the organization or consent (*)

For professionals (by electronic means, post or telephone)

Electronically, for similar goods and services already purchased/subscribed from the data controller

(*) In accordance with the GDPR, it is up to the data controller to determine, depending on the characteristics of the processing implemented, the most appropriate legal basis.5. Personal data concerned

The organization shall only collect and use data that is relevant and necessary to its business management needs. This may be data relating to: a) The identification of the data subject;

The internal code used to identify the person concerned in the database cannot be their bank card number, nor their social security number, nor even that of their identity document.

If the organization must ensure the identity of a person before entering into a commercial relationship with them, the simple consultation of proof (identity document) may be sufficient. When the law provides for it or if the organization justifies needing it to pre-constitute evidence in the event of litigation, and this according to the risks of litigation, a copy of this proof may be kept for a maximum period of 6 year. In this case, reinforced security measures such as, for example, the limitation of the quality of the digitized image or the integration of a watermark bearing the date of collection and the identity of the organization, must be put in place. implemented to combat the risks of misuse of this information, in particular the use of photographs for facial recognition purposes. Similarly, this information must not be kept in an active database but must be stored in an intermediate archiving database. b) For professional life; c) For the means of payment used, i.e. the strictly necessary data for the execution of a payment, more precisely the data relating to the bank card (number, end of validity, visual cryptogram, RIB) or to the check; d) The goods or services subscribed (data related to the payment of invoices, the follow-up of the commercial relationship, the opinions left, the management of complaints, etc.).

When the good purchased or the service subscribed involves, for example, the processing of health data or data directly relating to sexual orientation, the consent of the persons is required. For example, a dating site that requires you to enter your sexual orientation or a mobile application that collects health data should first obtain the consent of people wishing to register.

The nature of the goods or services consumed by a person should not be used to deduce information concerning them that may fall under the category of so-called "sensitive" data (alleged racial origin or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning sex life or sexual orientation). In any case, any categorization or creation of segments on the basis of such data, for the purposes of creating such a profile and/or sending

personalized advertising, must meet a legitimate purpose (Article 5 of the GDPR) and be subject to obtaining the prior consent of the customer concerned. e) The family, economic and financial situation of the person(s) concerned by the transaction when such data is linked to the commercial relationship.

A table below lists the main data that can be collected and processed by the organization. In application of the principle of data minimization, only those which are necessary for the implementation of the purpose envisaged by the commercial management processing can be collected (see point 3). The minimization of data favors, in particular, the preservation of accurate and up-to-date data. After having ensured the necessity and the relevance of the personal data that it uses, the organization must take all reasonable measures to guarantee the quality of the data it processes, in order to ensure its accuracy, throughout the lifetime of the processing.

PRACTICAL AND NON-EXHAUSTIVE ILLUSTRATION OF DATA THAT MAY BE COLLECTED Identity

Civility, surname, first names, address (including place of invoicing), telephone number, fax number, e-mail addresses, date of birth, internal processing code allowing the identification of the customer, accounting identification code .

The internal code allowing identification cannot be the number of bank card, social security, or identity document.

If a copy of an identity document is collected, reinforced security measures, such as, for example, the limitation of the quality of the digitized image, the integration of a watermark bearing the date of collection and the identity of the data controller, can be implemented in order to guard against the risks of misuse of this information and, for example, of the use of the photographs that these documents include for facial recognition purposes.Personal situation

Marital life, number of people in the household, number and age of the child(ren) in the household, profession, field of activity, socio-professional category, presence of pets.

The collection of sensitive data (i.e. data likely to reveal an alleged racial or ethnic origin, political, philosophical or religious opinions, trade union membership, sexual orientation or information on the health of the data subject), subject to having obtained the consent of the person concerned.Professional life

Profession, economic category, activity. Settlement / Payment

Data relating to the bank card (number, expiry date, visual cryptogram), transfer (RIB) or check.

Visual cryptogram of the bank card, which must systematically be deleted once the transaction has been carried out.

Discounts granted, receipts, balances, credits subscribed (amount and duration, name of the lender) in the event of financing

of the order by credit.Transaction

Transaction number, details of the purchase, subscription, good or service subscribed. Follow-up of the relationship commercial

Documentation requests, trial requests, articles, product purchased, service or subscription taken out, services covered by the order and the invoice, quantity, amount, frequency, date and amount of the order and the invoice, expiry date of the invoice, delivery conditions and address, history of purchases and services, return of products, origin of the sale (seller, representative, partner, affiliate).

Orders, invoices, correspondence with the customer and after-sales service, exchanges and comments from customers and prospects, person(s) in charge of customer relations.

Data relating to the contributions of persons who submit opinions on products, services or content, in particular their pseudonym.6. Users and recipients of information

In order to comply with the obligation of data security, personal data must be made accessible only to persons authorized to know it with regard to their attributions within the company's internal departments, departments responsible for controls or with the subcontractors.

The achievement of some of the purposes covered by this reference system may justify the transmission of data to third parties (postal services, research or communication offices, accounting bodies, etc.). Depending on the case, these recipients will have the status of data processor or will be fully responsible for processing the data received. respectively incumbent on each of the parties with regard to data protection (Article 28 of the GDPR). The data controller must document the instructions that he sends to the subcontractor and which concern the methods of data processing (article 22 paragraph 3.a of the GDPR). The Subcontractor's Guide published by the CNIL specifies the nature of these obligations and the clauses that it is recommended to include in the contracts. Access authorizations should be documented and access to the various processing operations be subject to traceability measures (see point 10 relating to security). The transmission, for a fee or not, of personal data to partners (third parties wishing to reuse them for commercial purposes) must also comply with the following principles: - if the purpose of the transmission is to allow commercial partners to carry out prospecting on the basis of their legitimate interest (non-electronic prospecting):

* it can itself be carried out on the basis of legitimate interest;

* the organization transmitting the data must inform the persons concerned, on the data collection medium (online form or paper form) of the purpose of this transmission and the categories of partners made recipients of the data. With a view to transparency, an exhaustive list of recipients, including their identity, could be regularly updated and made available to the persons concerned from this same medium (for example, by including a hypertext link). This second level of information can also usefully indicate how to find out about the data protection policy of each business partner;

* the organization transmitting the data must offer the persons concerned, in an express and unambiguous manner, the possibility of opposing, free of charge and in a simple manner, the transmission of their personal data at the time when they these are collected and at any time; - if the purpose of the transmission is to allow business partners to carry out prospecting requiring the collection of the prior consent of the persons concerned (electronic prospecting):

* in view of the fact that commercial prospecting by electronic means presents specific risks (in particular by the volume of requests likely to be received due to its automation), the organization transmitting the data must inform the persons concerned, on the medium data collection (online form or paper form), and obtain their consent to this transmission;

* the organization transmitting the data must, beforehand, have allowed the persons concerned to appreciate the consequences of their choice as regards the transmission by informing them of the extent of the latter. Highlighting to the data subjects the number and sector of activity of the partners who would be recipients of the data is an example of a measure that contributes to respecting the reasonable expectations of the data subjects in this regard;

* before carrying out prospecting by electronic means, the partners made recipients of the data must prove that they also have the consent of the people who will be canvassed. In the absence of such consent, the processing of commercial prospecting by electronic means is unlawful.

=> in this respect, the Commission recommends that the organizations transmitting the data obtain this consent, on behalf of the recipients, at the time of the initial collection of the data. To do this, individuals must be informed of the identity of the partners in charge of processing who would use their data for prospecting purposes, by means of an exhaustive list made available directly on or from the collection medium (for example , by including a hypertext link), as well as the specific purpose of the transmission;

=> in such a case, the organizations transmitting the data can use a single checkbox to obtain the consent to the transmission of the data and that related to the future use of the data, subject to providing complete prior information such as than described

above;

* when the organization collecting and transmitting the data has not obtained consent for the recipient, the latter must guarantee the lawfulness of its prospecting operations by electronic means, by obtaining the consent of the persons concerned beforehand;

=> in this respect the Commission considers that the solicitation operation by which the purchaser of the database offers people to receive commercial offers electronically is itself a processing of this data, which may be based on its legitimate interest;

=> as such, in order to verify whether such an operation falls within the reasonable expectations of the persons concerned, it is in particular the responsibility of the partner to ensure that the persons concerned have received sufficient information when transmitting their data (for example on the type of request, the approximate number of partners, the sectors concerned, and the duration during which the data controller will be authorized to transmit the data);

=> in any case, the number of requests addressed to the same person concerned should be limited since the people do not expect to receive multiple requests which can constitute a significant nuisance;

=> the partner must also ensure that the request for consent sent is not itself comparable to a form of commercial prospecting, subject, by its content and its mode of transmission, to the prior consent regime provided for by the article L. 34-5 of the CPCE. Therefore, if sent electronically, the message requesting consent must not promote the recipient's image or the goods and services that he sells.

In all cases, the consent of the persons must be kept as evidence and the use of pre-ticked boxes is not allowed to collect the consent of the persons concerned.

Finally, in general:- the partners made recipients of the data must, during the first communication with the persons concerned, inform them of all the information provided for in Article 14 of the GDPR, such as how to exercise their rights , and in particular the right of opposition, as well as the source from which the data used come;

- the organization transmitting the data is required to notify the partners to whom the personal data have been communicated, of any request for erasure or limitation of processing expressed by the persons concerned.

To ensure the continuity of the protection of personal data, transfers of this data outside the European Union are subject to special rules. Thus, any transmission of data outside the EU must, in accordance with the GDPR:

- be based on an adequacy decision; Where

- be governed by internal company rules, standard data protection clauses, a code of conduct or a certification mechanism approved by the CNIL; Where

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

- or meet one of the derogations provided for in Article 49 of the GDPR.7. Storage periods

A retention period must be set according to each purpose. In general, retention periods should not, in principle, exceed the durations of legal prescriptions.

The repository proposes retention periods. An organization can choose to deviate from the repository and choose to keep the data for a longer period; he must then ensure that this duration does not exceed that necessary with regard to the purposes for which they are processed (article 6 of the GDPR).

The visual cryptogram of the credit card must be deleted as soon as the payment for the service or the purchase is finalized, on the one hand because it is no longer necessary once the purchase is finalized and, on the other hand , because its retention creates security risks. On the other hand, the number of a payment card may be kept to allow subsequent purchases under the conditions laid down by the recommendation relating to the processing of the payment card for the sale of goods or the provision of services remotely (deliberation n ° 2018-303 of September 6, 2018). The data necessary for the execution of contracts are kept for the duration of the contractual relationship.

At the end of the contract, they must be kept in intermediate archiving and for a reasonable period, if the data controller has a legal obligation to do so (for example, to meet accounting or tax obligations) or if he wishes to constitute a evidence in the event of litigation, and within the limit of the applicable limitation period. A dedicated archive database or a logical separation in the active database should be provided for this purpose, after sorting the relevant data to be archived. In these cases, the data is processed for a purpose other than the performance of the contract and must, in accordance with the GDPR, be based on another legal basis, such as the legitimate interest provided for in Article 6.1.f or the obligation provided for in Article 6.1.c.

Customer data used for commercial prospecting purposes may be kept during the commercial relationship, then for a period of three years from the end of the commercial relationship (for example, at from a purchase, the expiry date of a warranty, the end of a service contract or the last contact from the customer).

Personal data relating to a non-customer prospect may be kept for a period of three years from their collection by the data

controller or the last contact from the prospect (for example, a request for documentation or a click on a hypertext link contained in an e-mail referring to the promoted product; on the other hand, the simple opening of an e-mail should not be considered as a contact emanating from the prospect).

At the end of this three-year period, the data controller may contact the data subject again to find out if he wishes to continue to receive commercial solicitations. In the absence of a positive and explicit response from the person, the data should be deleted or archived for a period in accordance with the provisions in force.

For commercial activities that involve the creation of an online account by customers (for example, dating sites or social networks), the data may be retained until the account is deleted by the user. However, it is common for users to no longer use these accounts without deleting them, which leads to these accounts persisting indefinitely. In this case, the organization should determine a reasonable period after which the account will be considered inactive and must therefore be deleted. In this respect, a period of two years seems proportionate. Finally, the users concerned may be notified before the expiry of this period in order to give them the possibility of expressing their wish to keep their account active.

When a person exercises their rights, the data collected in this context, such as information relating to the request of the person concerned, may be kept until the data controller responds to the request and in compliance with the principle of minimization provided for in Article 5.1.c. of the GDPR. The response provided may be kept for the purposes of proof, within the limit of the applicable limitation period, from the moment the data controller responds to the request.

Finally, the collection of supporting documents of identity in the context of the exercise of rights is only possible when there is a reasonable doubt as to the identity of the person, in accordance with Article 12.6 of the GDPR. In principle, these must be deleted as soon as the request of the data subject has been granted. Indeed, the provision of such documents has the sole purpose of verifying the identity of the person from whom the request emanates and it is not necessary to keep them once the identity has been confirmed. However, it is possible to keep these documents for the purpose of establishing evidence in certain exceptional cases where the controller identifies a strong risk of litigation, according to a case-by-case and duly documented analysis. In this case, the retention period for the supporting documents is determined in accordance with the limitation periods for public action provided for in Articles 8 and 9 of the Code of Criminal Procedure. For more information, 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 the G29

guidelines on anonymisation).8. Information of people

The processing of personal data must be implemented in complete transparency vis-à-vis the persons concerned.

From the data collection stage, individuals must be informed of the methods of processing their data under the conditions provided for by the provisions of Articles 13 and 14 of the GDPR. See the information notice models on the CNIL website.

Depending on the purpose pursued and the data collected, the consent of the persons (for example: in the case of prospecting by electronic means) or a means of opposing certain processing operations (for example: prospecting for similar products or services, canvassing between professionals or by post) must also be provided for on the data collection form.

In accordance with the GDPR, data subjects must also be informed of how to exercise their rights.9. Rights of persons

Data subjects have the following rights, which they exercise under the conditions provided for by the GDPR:

- right to withdraw their consent or oppose the processing of their data;

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

- 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 it carries out the necessary checks);

- 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 the data provided by the person on the basis of his consent or a contract are concerned. It is therefore recommended to inform people of the processing covered by this right to portability.

In accordance with Article 21 of the GDPR, if the legal basis of the processing is the legitimate interest, the persons concerned have a right of opposition, unless the organization demonstrates that there are legitimate and compelling reasons for processing that prevails over the interests and rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.

Consideration of the opposition request in such a case must however be systematic if it relates to data subject to commercial prospecting processing.

To facilitate the exercise of rights, the CNIL recommends that the organization make available to the persons concerned, at a minimum, a dedicated email address and/or the contact details of the data protection officer (DPD/DPO) of the 'organization.

The establishment of a dedicated channel for receiving requests to exercise rights does not exempt the organization from its

obligation to process requests addressed to it through other channels.

Any organization wishing to implement commercial prospecting by telephone must remove from its list the persons registered on the opposition list provided for by the provisions of Articles L. 223-1 and following of the Consumer Code (list known as "BLOCTEL "), without prejudice to legal exceptions.10. SecurityThe organization must take, in accordance with the GDPR, all the 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 storage, to prevent them from being deformed, damaged or that unauthorized third parties have access to it.

In particular, in the specific context of this standard, the organization is invited to adopt the following measures, to justify their equivalence or the fact of not needing or not being able to use them:

Categories

Measures

Educate users

Inform and educate people accessing the data.

Draft an IT charter and give it binding force.

Authenticate users

Define an identifier (login) specific to each user.

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

Force user to change password after reset.

Do not store passwords in plain text.

Limit the number of attempts to access an account.

Manage authorizations

Define authorization profiles.

Delete 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 to unlock smartphones.

Protect the internal computer network

Limit network flows to what is strictly necessary.

Securing the remote access of nomadic computing devices by VPN.

Implement WPA2 or WPA2-PSK protocols 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 username is embedded in the URLs.

Check that user input matches what is expected.

Collect consent for cookies not necessary for the service.

Back up and plan for business continuity

Perform regular backups.

Store backup media in a secure location away from the main site.

Provide security means for the transport of backups.

Plan for 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 specific clauses 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 sending it.

Make sure this is the correct recipient.

Transmit the secret through 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 default settings to end users.

Avoid free comment areas or strictly frame them.

Test on fictitious or anonymized data.

Use cryptographic functions

Use recognized algorithms, software and libraries.

Store secrets and cryptographic keys securely.

The organization whose processing fulfills the conditions set by these standards must ensure that the processing complies with the appropriate level of security required by Article 32 of the GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks posed by the processing, the degree of likelihood and severity of which vary for the rights and freedoms of natural persons.

To do this, the organization may usefully refer to the Personal Data Security Guide.11. Data Protection Impact Assessment

Pursuant to Article 35 of the GDPR, the data controller must carry out a data protection impact assessment (DPIA) when the processing it implements is likely to present a high risk to data subjects. rights and freedoms of data subjects.

First of all, it is advisable to refer to the lists published by the CNIL relating to the processing likely or not to be systematically the subject of a DPIA, namely: the list of processing for which an impact analysis is not not required; then the list of processing operations for which an impact analysis is required.

With regard to the latter, there are in particular the following type of processing operations:

Type of processing operations

Non-exhaustive examples

Large-scale location data processing

- Mobile application to collect the geolocation data of its users;

- provision of an urban mobility geolocation service used by a large number of people;

- "customer" database of electronic communication operators.

If the processing implemented is not present on one of these lists, the data controller must consider the need to carry out a DPIA. For this purpose, the criteria established by the European Data Protection Board (EDPB) in its guidelines should be consulted. These provide that the completion of a DPIA is mandatory when at least two of the nine criteria below are met:

- evaluation or rating of a person;

- automated decision-making;

- systematic monitoring;

- processing of sensitive or highly personal data;

- large-scale processing;

- 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.

In order to carry out a DPIA, the data controller may use:

- the principles contained in this reference system;

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

If the organization has appointed a data protection officer (DPD/DPO), the latter must be consulted.

In accordance with article 36 of the GDPR, the data controller must consult the CNIL before any implementation of its processing if the impact analysis indicates that it does not manage to identify sufficient measures to reduce the risks to a acceptable level.

The president,

M. L. Denis