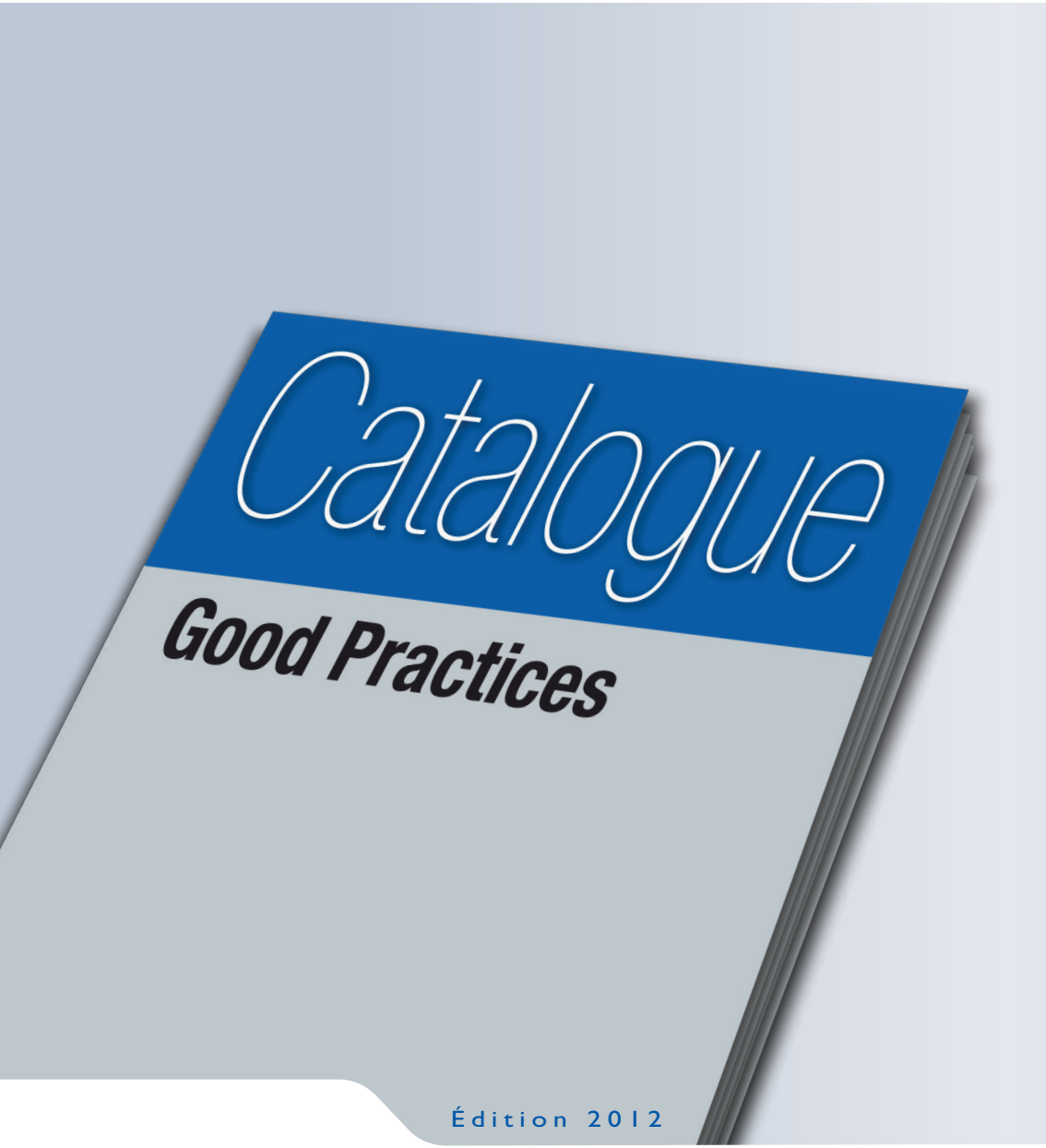
MEASURES FOR THE PRIVACY RISK TREATMENT



Édition 2012

CNIL
Commission Nationale de l'Informatique et des Libertés

Contents

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

METHODOLOGY OF TRANSLATION

As a principle, it was decided not to translate the original titles of French institutions or procedures which appear in the text, when their translation may be misleading.

For example, the title of the "Commission Nationale de l'Informatique et des Libertés" (CNIL), the French Data Protection Authority, was not translated and it appears as such or under its acronym (CNIL) in the body of the text.

It has been decided not to translate the references tag [example] when the referred document was not available in English.

This English version of "*Gérer les risques sur les libertés et la vie privée, la méthode"* **is provided for informative purposes, only as a courtesy for the non-French reading public. While the CNIL has tried to provide an accurate translation of the original guide available in French, in case of discrepancies between the two texts, the French version shall prevail.**

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Foreword

This document is a catalogue of good practices intended to treat risks that the processing of personal data may pose to the civil liberties and privacy of data subjects. It supplements the risk management method of the *Commission Nationale de l'Informatique et des Libertés* (CNIL, the French data protection authority) with regard to risks to civil liberties and privacy and helps to determine the measures proportionate to the risks identified using this method.

It is not limited to technical considerations of computer systems, but applies to information systems comprehensively, from those systems to persons, paper documents, organization and premises.

***Warning:* this document is not exhaustive and is updated regularly. In addition, the measures must be chosen based on the risks identified to develop a comprehensive, consistent system that includes other measures. Last, they should be adapted to the context of the particular treatment.**

This catalogue is intended primary for data controllers and, in particular, for stakeholders involved in creating and improving personal data processing:

- project owners and their advisors, who must conduct a prior assessment of risks to their system and define the security objectives;
- prime contractors and their advisors, who must propose solutions to treat risks identified pursuant to the objectives identified by project owners;
- privacy officers, who must support project owners in the area of personal data protection and interface with the CNIL;
- chief information security officers (CISO), who must support project owners in the area of information systems security (ISS) by complying with civil liberties and privacy.

The goal of this catalogue is to help them implement the [Act-I&L] in connection with the processing operations they perform. To that end, it must:

- enable them to select measures proportionate to the risks (necessary and sufficient to treat the risks identified);
- provide them with actionable examples; and,
- offer them guidance in reaching a deeper understanding of these issues.

Note: the wording in brackets ([text]) refers to the normative and bibliographic references in the appendix to the document.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1. Protecting primary assets

1.1. Minimizing the amount of personal data

Objective: to reduce the severity of risks by limiting the amount of personal data to what is strictly necessary to achieve a defined purpose, pursuant to Article 6 of the [Act-I&L].

The lawfulness of personal data

"Processing may be performed only on personal data that meet the following conditions:
1° the data shall be obtained and processed fairly and lawfully;
2° the data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. However, further data processing for statistical, scientific and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is carried out in conformity with the principles and procedures provided for in this Chapter, in Chapter IV (formalities prior to commencing data processing) and in Section 1 of Chapter V (obligations incumbent upon the data controllers and the rights of individuals) as well as in Chapters IX (processing of personal data for the purpose of medical research) and X (processing of personal medical data for the purposes of evaluation or analysis of care and prevention practices or activities) and if it is not used to take decisions with respect to the data subjects;
3° they shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing;
4° they shall be accurate, complete and, where necessary, kept up-to-date. Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and incomplete with regard to the purposes for which they are obtained and processed;
5° they shall be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed."

(Article 6 of the [Act-I&L])

Good practices when the measure is selected to treat the risks

- Confirm that the personal data is sufficient, relevant and not excessive with regard to the intended purpose; otherwise, do not collect the data.
  - *Recommendations: define the purpose of the processing, identify the personal data necessary to achieve that purpose, demonstrate why each category of personal data is critical and, last, rule out any personal data that does not prevent the purpose from being achieved; if necessary, review the purpose if the data are necessary for something other than the initial intended purpose.*

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- Confirm that the personal data do not reveal (directly or indirectly) racial or ethnic origin, political, philosophical or religious views, trade union membership, health information or information on an individual's sex life and do not collect them if they do, except under exceptional circumstances (for example, with consent, in the public interest or pursuant to Article 8 of the [Act-I&L]).
- Confirm that the personal data do not relate to offenses, criminal convictions or security measures and do not collect them if they do, except under exceptional circumstances (for example, in dealing with the courts or court officers).
- Prevent the collection of additional personal data.
    - *Recommendations: only fields that relate to the personal data defined are to be created and may be entered in a database. No additional field may be added (do not include a "free text field"). Check regularly to ensure that no additional personal data is collected in relation to the data initially identified.*
- Restrict the transmission of electronic documents containing personal data to the individuals who need them in connection with their work.
- Securely delete personal data that are no longer useful or that a subject requests be deleted from the system in operation or from back-ups, if necessary.
    - *Recommendations: use a secure deletion tool for electronic documents and a degaussing device for storage units that use magnetic technologies.*

Tools/For further information

- See the [ANSSI-Effacement] guide and the certified secure deletion software.[1]

Note

- Some categories of data are subject to specific restrictions (in particular, sensitive data within the meaning of Article 8 and data under Article 9[2] of the [Act-I&L]).

[1] See the list of products that have received first-level security certification (CSPN): http://www.ssi.gouv.fr/site_rubrique54.html.

[2] Only certain categories of legal entities may process data "regarding offenses, criminal convictions and security measures."

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.2. Managing personal data retention periods

Objective: to reduce the severity of risks by ensuring that personal data is not retained for longer than necessary, pursuant to Articles 6 and 35 of the [Act-I&L].

Good practices when the measure is selected to treat the risks

- Define personal data retention periods that are time-limited and appropriate to the purpose of the processing.
- Confirm that the processing can detect the expiration of the retention period.
  - *Recommendations: the processing should incorporate the date when each piece of personal data recorded should be deleted.*
- Confirm that the processing allows the deletion of personal data when the retention period expires and that the method chosen to delete them is appropriate to the risks to the civil liberties and privacy of the data subjects.
  - *Recommendations: if the risks are low, personal data may simply be deleted; if the risks are high, secure deletion tools should be used.*
- When the retention period expires, delete the personal data promptly.
  - *Recommendations: develop an automated functionality that erases personal data when their retention period expires.*

Note

- In general, the purpose of the processing does not justify retaining personal data in anticipation of police or court action for a period longer than provided for in the [Act-I&L]. However, certain sectors are required to retain certain data for a defined period (for example, telecommunications operators and airline passengers).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.3. Informing data subjects

Objective: to ensure that the subjects are informed, pursuant to Article 32 of the [Act-I&L].

Good practices when the measure is selected to treat the risks

- Confirm that the processing is not covered by an exception and is not subject to the specific conditions set forth in Article 32 of the [Act-I&L] (electronic communications networks user, statistics, anonymization, national security, defense, public safety, enforcement of criminal sentences, security measures, prevention, research, findings and prosecution of criminal offenses).
- Determine the practical means that will be implemented to inform the data subjects.
- Ensure that the notification is complete, clear and appropriate to the target audience based on the nature of the personal data and the practical means chosen.
    - *Recommendations: present the information in clear language that can be understood by a person who is not familiar with information technologies or the Internet.*
- Ensure that the notification is provided by the time the data is collected.
- Ensure that the data cannot be collected without providing this information.
    - *Recommendations: Determine alternative solutions in the event that the practical means are no longer operational.*
- If possible, provide a means by which to show that notification was provided.
    - *Recommendations: post this information on a sign that all employees must see or require that a notice or document be signed or initialed.*

Notes

- The notification must be delivered individually (for example, in a verbal exchange or a pop-up window), but may be done collectively (by note or poster in a premises) if the data controller is sure that all data subjects will have easy access to this method.
- The notification must include the identity of the data controller, the purpose of the processing, whether the information collected is required or optional, the consequences for failing to respond, the recipients of the information, the subject's rights, the person responsible for enforcing the rights and the projected transfers of the data.

Tools/For further information

- See Article 32 of the [Act-I&L] for the content of the notification, exceptions and specific conditions.
- See the model legal notices on the CNIL site.[3]

[3] See http://www.cnil.fr/vos-responsabilites/informations-legales.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.3.1 Employees of an organization

Good practices when the measure is selected to treat the risks

- Obtain the prior opinion of the employee representative organizations in the cases set forth in the Labor Code.
- Use the method that is most appropriate to the organization.
  - *Recommendations: posters, internal memos, email, specific forms, labor contract, internal regulations or the IT charter.*

1.3.2 Collecting personal data via an Internet site

Good practices when the measure is selected to treat the risks

- Provide direct or easily accessible information for Internet users.
  - *Recommendations: post or provide access to information on the home page or on the section of the site or service used that deals with compliance with privacy provisions.*

1.3.3 Collecting personal data by telephone

Good practices when the measure is selected to treat the risks

- Deliver an automatic message before the conversation begins with information on subjects' rights, the reason for recording the conversation (for training purposes or to monitor service quality), if necessary, and an opportunity to refuse recording (on legitimate grounds).
- Establish methods by which to authenticate the caller (for example, by providing information known only to the organization and the subject).

1.3.4 Collecting data via a form

Good practices when the measure is selected to treat the risks

- Place the appropriate notice on the form in a typeface identical to the rest of the document.

1.3.5 Using targeted advertising techniques

Good practices when the measure is selected to treat the risks

- Make the information available to Internet users in visible, legible form.
- Inform Internet users about the various forms of targeted advertising they are likely to see via the service they are accessing and the various procedures used, the categories of information processed to adapt the advertising content and, as needed, the information that is not gathered and how they may agree to the display of behavioral or personalized advertising. Notification must be provided and consent obtained before any information is stored or before accessing information already stored in the terminal equipment.

Tools/For further information

- See the opinion [G29-Advertising].

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.3.6 Updating existing processing

Good practices when the measure is selected to treat the risks

- Provide specific notification about new forms of processing (for example, new purposes or new recipients).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.4. Obtaining the consent of data subjects

Objective: to allow data subjects to make a free, specific and informed choice, pursuant to Article 7 of the [Act-I&L].

Good practices when the measure is selected to treat the risks

- Determine whether the processing relies on a legal basis other than consent, as set forth in Article 7 of the [Act-I&L] (including legal obligation, protection of life, public service mission, contract or measures taken with the individual and legitimate interest).
- Determine the practical means to be implemented to obtain the consent of the data subjects.
- Ensure that consent is obtained before any processing begins.
  - *Recommendations: analyze the cases where the practical means chosen are no longer operational and determine emergency solutions, if necessary.*
- Ensure that consent is obtained freely.
  - *Recommendations: confirm that an alternative exists that is not overly restrictive (it must provide a choice) and that no hierarchical relationship exists (for example, between an employee and his/her employer).*
- Ensure that the consent is obtained in an informed, transparent manner in terms of the purposes of the processing.
- Ensure that consent is obtained for a specific purpose.
- When subcontracting is involved, set out each party's obligations in an explicit written agreement accepted by both parties.

Tools/For further information

- See Article 32. II of the [Act-I&L].
- See Article L. 34-5 of the Postal and Electronic Communications Code regarding the provisions specific to sales prospecting.

Notes

- The CNIL considers that an employee cannot consent freely to processing set up by his/her employer given their hierarchical relationship.
- The practical means for obtaining consent include actions that an individual must perform (for example, entering a PIN,[4] placing a cellphone close to a smart poster when advertisements are sent from a smart poster to a telephone via Bluetooth or requiring that an NFC[5] peripheral be placed close to a reader).

[4] Personal Identification Number.
[5] Near Field Communication.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.4.1 Data falling under Article 8 of the [Act-I&L]

Objective: to allow free, specific and informed choice regarding data on racial or ethnic origins, political, philosophical or religious opinions, membership in a trade union or the subjects' health or sex life.

Good practices when the measure is selected to treat the risks

- Obtain the informed, express consent of data subjects prior to initiating the processing, unless the processing relies on a different legal basis or if the law prohibits collecting or processing personal data.

1.4.2 Collecting personal data via an Internet site

Good practices when the measure is selected to treat the risks

- Provide a form with boxes that must be checked and that are not checked by default ("opt-in" approach).

1.4.3 Collecting personal data via cookies

Good practices when the measure is selected to treat the risks

- If a cookie is not strictly necessary to provide the service that the user has expressly requested, obtain the Internet user's consent (for example, via a banner at the top of a web page[6] or a consent request zone overlaid on the page or boxes and that must be checked when subscribing to a service online) after informing the user and before storing the cookie.
    - *Recommendations: ensure that the information is written in simple, but precise, language understandable to the general public (for example, if the purpose of the cookie is to "create user profiles in order to send targeted advertising," the information should use all those terms and not simply refer to "advertising."*

Notes

- In order for free and specific consent to be communicated via the browser settings, the browser must allow the user to choose which cookies to accept and for what purpose. A browser that accepts all cookies by default and does not distinguish their purpose cannot be considered as allowing the user to provide valid consent because it would not be specific.

Tools/For further information

- See the information sheet, "What the Telecoms Package Changes for Cookies" on the CNIL website.[7]

[6] Solution used on the site www.ico.gov.uk.
[7] http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.4.4 Geolocation via a smartphone

Good practices when the measure is selected to treat the risks

- Enable users to refuse to allow an application to systematically geolocate them.
- Allow users to choose which application may use geolocation.
- Allow users to choose the persons authorized to access their geolocation information and at what level of detail.

1.4.5 Using targeted advertising techniques

Good practices when the measure is selected to treat the risks

- Provide users simple, no-cost methods to accept or refuse advertising based on their navigation behavior and to choose the targeted advertising they would like to receive based on their interests.
    - *Recommendations: provide Internet users a platform from which to accept or refuse, completely or in part, the display of targeted behavioral advertising; explain how to delete cookies and browser histories, authorize or prohibit the storage of cookies; and allow cookies to be created and stored showing that the user has chosen not to receive behavioral advertising from third parties.*

1.4.6 Research that uses identifiable biological samples[8]

Good practices when the measure is selected to treat the risks

- If the samples are preserved for further processing that is different from the initial processing, also be sure to obtain the data subject's express, informed consent to this other processing.

[8] For example, DNA.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.5. Permitting the exercise of the right to object

Objective: to ensure that individuals have an opportunity to object to the use of their personal data, pursuant to Article 38 of the [Act-I&L].

Good practices when the measure is selected to treat the risks

- Confirm that the processing is not covered by an exception in Article 38 of the [Act-I&L] (legal requirement or exclusion noted in the act establishing the processing) that prohibits the individual from objecting to the processing.
- Determine the practical means that will be implemented to allow individuals to exercise the right to object. They must be able to exercise this right as quickly as possible, within a period not to exceed two months, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage individuals from objecting and must not involve any cost to them.
- Ensure that the right to object may always be exercised and that the personal data collected and processed actually allow the exercise of the right to object.
    - *Recommendations: analyze the cases where the practical means chosen are no longer operational and identify back-up solutions, if necessary.*
- Ensure that "the interested party is able to express his or her choice prior to the final validation of his or her responses," pursuant to Article 96 of the [Decree-I&L].
    - *Recommendations: confirm that the right to object may be exercised before the data subjects provide final validation of their responses or before the collection is completed.*
- Confirm that requests to exercise the right to object submitted on site provided for verification of the identity of the individuals submitting requests and the identity of the individuals they may appoint as their representative.
- Confirm that requests to exercise the right to object submitted by regular mail are signed and accompanied by a photocopy of a piece of identification (which should not be retained unless proof must be kept) and that they specify a reply-to address.
- Confirm that requests to exercise the right to object submitted by email (using an encrypted channel if transmitted via the Internet) include a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file).
- Ensure that individuals exercising their right to object provide legitimate grounds and that those grounds are evaluated (except in the case of marketing and processing for the purpose of health research falling under Chapter IX of the [Act-I&L], which provides the individual a discretionary right to object).
- Ensure that all recipients of the processing are notified of the objections submitted by the data subjects, pursuant to Article 97 of the [Decree-I&L].

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.5.1 Processing via telephone

Good practices when the measure is selected to treat the risks

- Provide a mechanism allowing data subjects to express their opposition by telephone.
    - *Recommendations: allow an objection to be expressed by pressing a telephone button.*

1.5.2 Processing via electronic form

Good practices when the measure is selected to treat the risks

- Create an easily accessible form with opt-out boxes to check or allow the user to unsubscribe from a service (delete an account).

1.5.3 Processing via electronic mail

Good practices when the measure is selected to treat the risks

- Ensure that the sender of the messages is clearly identified.
- Ensure that the body of the messages relates to the subject of the messages.
- Allow recipients to object by responding to the message or by clicking on a link. Individuals should not be required to identify themselves to unsubscribe.

1.5.4 Research using identifiable biological samples[9]

Good practices when the measure is selected to treat the risks

- If the samples are retained for further processing different than the initial processing, also allow the data subjects affected by the further processing to object, without requiring them to provide legitimate grounds.

[9] For example, DNA.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.6. Permitting the exercise of the direct access right

Objective: to ensure that individuals have an opportunity to know about their personal data, pursuant to Article 39 of the [Act-I&L].

Good practices when the measure is selected to treat the risks

- Confirm that the processing is not subject to an exception referred to in Articles 39 and 41 of the [Act-I&L] (such as data processed for statistical or research purposes when there is no risk of a privacy breach and the data are retained only as long as necessary for these purposes or for reasons of national security, defense or public safety).
- Determine the practical means that will be implemented to allow the exercise of the direct access right. Individuals must be able to exercise this right as quickly as possible, within a period not to exceed two months, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the data subjects and they must not incur expenses that exceed copying costs.
    - *Recommendations: establish a process to inform individuals submitting requests about the status of their request and the necessary processing (for example, by regular mail or email, noting that the request has been received and the date by which they can expect to receive a response). In the case of stored archives, there may be some leeway regarding the response date if the data controller informs the individual submitting the request of the problems and has provided a reasonable response time.*
- Ensure that the right of access can always be exercised.
    - *Recommendations: analyze the cases in which the practical means chosen are no longer operational and identify back-up solutions, if necessary.*
- Confirm that requests to exercise the right of access submitted on site provide the identity of the individuals submitting requests and the identity of the individuals they may appoint as their representative.
- Confirm that requests to exercise the right of access submitted by regular mail are signed and accompanied by a photocopy of a piece of identification (which should not be retained unless proof must be kept) and that they specify a reply-to address.
- Confirm that requests to exercise the right of access submitted by email (using an encrypted channel if transmitted via the Internet) are accompanied by a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file).
- Ensure that all information that data subjects may request can be provided while still protecting the personal data of third parties.

Tools/For further information

- See Articles 92 – 95 and 98 of the [Decree-I&L].
- See the [CNIL-Employeurs] guide.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.6.1 Accessing medical files

Good practices when the measure is selected to treat the risks

- Provide the information within eight days following the request and within two months if the information is more than five years old (as of the date on which the medical information was assembled).
- Allow those who hold parental rights (for minors) and legal representatives (for individuals subject to guardianship) to exercise the right of access, pursuant to Article 58 of the [Act-I&L].

Tools/For further information

- See [Décret-2002-637].

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.7. Allowing the exercise of the right to correct

Objective: to ensure that individuals may correct, add to, update, block or delete their personal data, pursuant to Article 40 of the [Act-I&L].

Good practices when the measure is selected to treat the risks

- Confirm that the processing is not covered by an exception in Article 41 of the [Act-I&L] (national security, defense or public safety).
- Determine the practical means that will be implemented to permit the exercise of the right to correct. Individuals must be able to exercise this right as quickly as possible, within a period not to exceed two months, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the data subjects and must not involve any cost to them.
- Ensure that the right to correct may always be exercised.
    - *Recommendations: analyze the cases in which the practical means chosen are no longer operational and identify back-up solutions, if necessary.*
- Ensure that the identity of individuals submitting requests will be verified.
    - *Recommendations: confirm that requests to exercise the right to correct submitted via postal mail are signed and accompanied by a photocopy of a piece of identification (which shall not be retained unless proof must be kept), and that requests submitted via email (using an encrypted channel if transmitted via the Internet) are accompanied by a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file) and that requests specify a reply-to address and confirm the identity of individuals submitting requests on site and of individuals they may appoint as their representatives or of heirs of a deceased individual.*
- Ensure the accuracy of the corrections requested.
- Ensure that the individuals submitting requests receive confirmation.
- Ensure that the third parties to whom the data may have been sent are informed of the corrections made.

Tools/For further information

- See Articles 92 – 95 and 99 – 100 of the [Decree-I&L].

1.7.1 On-line advertising

Good practices when the measure is selected to treat the risks

- Provide a way for individuals to access the areas of interest in their profile and a way to modify them. The individual's identity may be authenticated based on the information used to access his or her account or on the cookie (or equivalent) on his or her computer.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.8. Partitioning personal data

Objective: to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.

Good practices when the measure is selected to treat the risks

- Identify the personal data useful only to each business process.
    - *Recommendations: provide individuals with access only to the data they need. For example, do not provide the statistics department with access to first and last names.*
- Separate the data useful to each process in logical fashion.
    - *Recommendations: manage the different access rights according to the business processes (including payroll management, vacation request management and career advancement) and establish a dedicated IT environment for systems that process the most sensitive data.*
- Regularly confirm that personal data are partitioned effectively and that recipients and interconnections have not been added.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.9. Encrypting personal data

Objective: to make personal data unintelligible to anyone without access authorization.

Good practices when the measure is selected to treat the risks

- Determine what should be encrypted (including an entire hard disk, a container,[10] certain files, data from a database or a communication channel) based on the form in which personal data is stored, the risks identified and the performance required.[11]
- Choose the type of encryption (symmetric[12] or asymmetric[13]) based on the context and the risks identified.
- Adopt encryption solutions based on public algorithms known to be strong.
    - *Recommendations: use tools (including private key protection systems, encryption modules or decryption modules) that are certified, qualified or that have obtained first-level security certification from the French Network and Information Security Agency (ANSSI)[14] at the level of robustness expected.*
- Establish measures to ensure the availability, integrity and confidentiality of the information necessary to recover lost secrets (including administrator passwords and a recovery CD).

Tools/For further information

- See the requirements regarding the [RGS] "Confidentiality" function.

1.9.1 Symmetrical (conventional) encryption

Good practices when the measure is selected to treat the risks

- Use only one key for a single purpose.[15]
- Choose a mechanism recognized by the appropriate organizations and that provides security proof.
    - *Recommendations: use mechanisms that comply with the [RGS] (the French government's general security database), such as the AES algorithm,[16] use a processed block size equal to at least to 128 bits, a non-deterministic encryption scheme (such as a CBC mechanism[17] with a random initialization*

[10] A file may contain several files.
[11] The solutions may be combined if there are many risks or if the risks are high.
[12] Intended only for persons with a shared secret key.
[13] Intended only for persons chosen from among those with a known public key.
[14] Provided that at least one such reference is included in the catalogue of products that have obtained ANSSI qualification. Otherwise, the electronic certificate service provider seeking to obtain qualification for its range of authentication certificates must obtain an exemption from the ANSSI.
[15] Using a single key for more than one purpose (for example, to ensure integrity with an HMAC mechanism or ensure confidentiality with a different mechanism) causes many errors. However, this not does prohibit differentiating, locally, two keys from a single secret key provided that the diversification mechanism complies with the [RGS].
[16] Advanced Encryption Standard.
[17] Cipher-block chaining.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

vector), cryptographic keys of a length appropriate to the expected useful life (for example, at least 128 bits for confidentiality guaranteed until 2020) and that are not weak keys.[18]

- Formalize the key management system.
  - *Recommendations: draft a procedure.*

1.9.2 Asymmetric (public key) encryption

Good practices when the measure is selected to treat the risks

- Use only one key for a single purpose.[19]
- Choose a mechanism recognized by the appropriate entities and that provides security proof.
  - *Recommendations: use mechanisms that comply with the [RGS], such as the RSAES-OAEP,*[20] *use cryptographic keys of a length appropriate to the expected useful life (for example, at least 128 bits for confidentiality ensured until 2020).*
- Generate the keys pursuant to the [RGS].
  - *Recommendations: use a registered electronic certificate service provider*[21] *that complies with Version 1.0 of the [RGS] for encryption use.*
- Establish mechanisms to verify the electronic certificates.
  - *Recommendations: when an electronic certificate is received, confirm, at a minimum, that it includes an indication of purpose consistent with expectations, is valid and has not been revoked and that a proper certification chain exists at all levels.*
- Protect the security of the generation and use of keys that is consistent with their level in the key hierarchy.
  - *Recommendations: protect users' keys when stored (including restrictive rules governing access rights, password, chip and PIN card) and apply heightened security measures (for example, require that several of the holders of part of the secrets use the keys or store them in a safe deposit box) to the generation and use of a key management infrastructure's root keys (those that will be used to sign the other keys).*
- Formalize the key management system.
  - *Recommendations: develop a "certification policy" (CP)*[22] *that specifies the responsibilities, identification and authentication, certificate life-cycle*

[18] With DES, an example of a weak key would mean that by applying the encryption function to the encrypted message, the message could be retrieved as cleartext.
[19] Using the same key for more than one purpose (for example, to ensure authenticity with an electronic signature mechanism and to ensure authentication with a different one) causes many errors. However, this not does prohibit differentiating, locally, two keys from a single secret key provided that the diversification mechanism complies with the [RGS].
[20] RSA Encryption Scheme - Optimal Asymmetric Encryption Padding.
[21] See http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.
[22] Model certification policies are available on the ANSSI site (see Annexes A6-A12 of the RGS).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

operational requirements, non-technical and technical security measures, profiles of the certificates and revocation lists and compliance audits and other evaluations.

1.9.3 Encrypting the equipment

Objective: to make personal data unintelligible to anyone without access authorization in order to reduce the risks associated with the recovery of a piece of equipment (for example, a workstation, a server or removable media[23]).

Good practices when the measure is selected to treat the risks

- Encrypt data at the hardware level (surface of the hard disk) or at the operating system level (encryption of a partition or a container).
  - *Recommendations: use encryptable equipment, such as hard disks with SED technology[24] or software such as dem-crypt (Linux), FileVault (MacOS), TrueCyrpt 6.0a (Windows).*
- Choose systems that do not store keys on the equipment that will be encrypted.

1.9.4 Encrypting databases

Objective: to render the personal data unintelligible to anyone without access authorization so as to reduce the risks associated with the theft of the server, improper physical access to a workstation or the server and direct access to the server's data by an administrator.[25]

Good practices when the measure is selected to treat the risks

- Based on the risks identified, perform encryption at the database level or at the level of the application that accesses the database or certain data from a database.

1.9.5 Encrypting partitions or containers

Objective: to make personal data unintelligible to anyone without an authorization access in order to reduce the risks associated with the recovery of a piece of equipment (including a workstation, server or removable media), improper physical access to a workstation or the server and direct access to the server's data by an administrator.

Good practices when the measure is selected to treat the risks

- Encrypt the data at the operating system level (encrypt a partition or a container).
  - *Recommendations: use software such as TrueCrypt 6.0a or Zed! 4.0.*

[23] USB key, external hard disk, CD-ROM,DVD-ROM and back-up media.
[24] Self-Encrypted Drive.
[25] Without encryption, administrators have immediate access to all the data stored in the database and can search them. An administrator of a database that includes health data can thus easily search by social security number (NIR) or by first and last name and access the individual's medical file.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.9.6 Encrypting standalone files

Objective: to make personal data unintelligible to anyone without an access authorization in order to reduce the risks associated with the theft of a workstation or server, improper physical access to a workstation or server and direct access to the data by an administrator.

Good practices when the measure is selected to treat the risks

- Encrypt the stored files or the email attachments.
  - *Recommendations: use software such as ZoneCentral 3.1 or those that use the Security BOX Crypto 6.0 library, AxCrypt or Gnu Privacy Guard (GPG). otherwise, at the least, use a compression tool that allows encryption with a password, such as 7-Zip, which provides AES encryption, or an equipment solution such as a Bull Trustway PCI cryptographic card.*

1.9.7 Encrypting email

Objective: to make personal data included in emails unintelligible to anyone without an access authorization in order to reduce the risks associated with email interception.

Good practices when the measure is selected to treat the risks

- Encrypt email messages.
  - *Recommendations: use software such as Gnu Privacy Guard (GPG).*

1.9.8 Encrypting a communications channel

Objective: to make personal data unintelligible to anyone without an access authorization in order to reduce the risks associated with the interception of data flows.

Good practices when the measure is selected to treat the risks

- Encrypt the communications channel between an authenticated server and a remote client.
  - *Recommendations: use a service authentication certificate that complies with the [RGS], the TLS protocol,[26] formerly SSL[27] (consider requiring a password to use the private key and protecting access to it key via very restrictive access rights), SSH[28] to set up a secure tunnel (VPN[29]) or IP[30] (VPN-IPSec) encryption solutions.*

[26] Transport Layer Security.
[27] Secure Sockets Layer.
[28] Secure Shell.
[29] Virtual Private Network.
[30] See the list of qualified products: http://www.ssi.gouv.fr/fr/produits/produits-qualifies/.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

1.10. Anonymizing personal data

Objective: to remove identifying characteristics from personal data.[31]

Good practices when the measure is selected to treat the risks

- Determine what must be anonymized based on the context, the form in which the personal data are stored (including database fields or excerpts from texts) and the risks identified.
- Permanently anonymize[32] the data that require such anonymization based on the form of the data to be anonymized (including databases and textual records) and the risks identified.
- If that data cannot be anonymized permanently, choose tools (including partial deletion, hashing, key hashing and index) that most closely meet the functional needs.

Tools/For further information

- It may be useful to formalize the anonymization requirements in more detailed fashion in order to choose the appropriate tools: the robustness expected when dealing with inference attacks[33] based on the risks identified and the data subjects.[34]
- The CNIL has issued resolutions specific to certain cases. It may be helpful to confirm that the measures chosen are appropriate in terms of the Commission's recommendations. For example, the CNIL's opinion on the anonymization of judgments and decisions that are freely accessible on the Internet is formalized in Resolution 01-57 of 29 November 2001.

Notes

- "True" anonymization necessarily involves an (irreversible) loss of information. In some cases, simply deleting or blacking-out part of the data may achieve the desired objective.
- "Pseudonymization" may be defined as the replacement of a name by a pseudonym. In this process, data lose their identifying characteristics (in direct fashion). The data remain linked to the same person across multiple data records and information systems without revealing the individual's identity. It may be performed with or with the possibility of re-identifying names or identities (reversible or irreversible pseudonymization).
- It is still possible to correlate anonymized personal data, so an individual may be re-identified based on partial information when personal data is anonymized but not deleted. Original data can be linked to anonymized data when secrecy is compromised and the original data is not sufficiently complex.[35]

[31] That is, make it impossible to establish any connection between personal data and the natural person to whom it relates.
[32] The data are anonymized, preventing anyone from finding the original data.
[33] To limit inference attacks and attacks on encryption keys, anonymization keys may also be changed regularly.
[34] For example, the place and date of birth may sometimes be enough to positively identify someone.
[35] For example, there are a limited number of French surnames (fewer than 1.5 million) and they are all indexed.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- Anonymization as a good security practice must be distinguished from the "anonymization process" within the meaning of the [Act-I&L], specifically Articles 8-III, 11-3 and 32-IV. As a general rule, in order for the CNIL to conclude that an "anonymization process" complies with the law, true anonymization must be carried out by deleting data or performing a "pseudonymization," together with strong organizational and technical guarantees, particularly by using keyed-hash functions.

1.10.1 Databases

Good practices when the measure is selected to treat the risks

- Perform irreversible anonymization of personal data where possible.
  - *Recommendations: delete a sufficient portion of the data (for example: keep only the year of birth, not the full date of birth, so that a person cannot be identified if his or her place of birth and gender are also known; delete the last two octets of an Ipv4 address; use a keyed-hash function and delete the secret key(s); or replace the identifying personal data by neutral text (stars, a few identical letters or a sequential identifier).*
- If this is not possible, determine the solutions that will best meet the functional needs.
  - *Recommendations:*
    - *if the authorized persons must be able to confirm that the anonymized data correspond to the original data in their possession, use an SHA-256 hash function with a secret key[36] (HMAC[37]) or perform a double anonymization with two secret keys held by two different organizations;[38]*
    - *if the authorized persons must be able to find the original data (lifting anonymity), use an encryption function, possibly by dividing a key into three components entrusted to three different persons (for example, on a CD or a smart card), requiring that at least two of the three meet to reconstitute the key in order to protect the confidentiality of the secret.*
- Use only anonymized personal data or fictitious data for the development and test phases.
  - *Recommendations: use specialized software to create anonymized sets of tests.*

Notes

- Determine the technical and organizational measures for protecting secrets (including keys and tables of correspondence) that allow the lifting of anonymity, if necessary,

[36] Be sure to protect the secret key, which can be used to find the hashed data corresponding to an identity.
[37] Keyed-Hashing for Message Authentication.
[38] A double reversible anonymization involves applying a second anonymization to the result of a first. Both anonymizations must use different secrets, held by separate organizations. The FOIN algorithm (nominative information occulation function) is an example of a double anonymization.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

ensuring that only the person holding the secrets may do so (including by separating and storing keys in fireproof chests and keeping an access log).

- In some cases, double anonymization is recommended: that is, use a second anonymization on the originally anonymized data. Both anonymizations must use different secrets, held by separate organizations.

Tools/For further information

- See [ISO-25237] and [AFNOR-97-560].
- See the requirements regarding the [RGS] cryptographic mechanisms.

1.10.2 Electronic textual records

Good practices when the measure is selected to treat the risks

- Use an anonymization system that complies with the [AFCDP-Anonymisation] reference framework.
- Manually confirm the anonymized records using the system selected in order to correct any anomalies and improve the system settings.

Tools/For further information

- See the [CNIL-DiffJurisprudence] resolution.
- Several software tools can identify and anonymize personal data (E-DOC LABS anonymization assistant, Temis' Insight Discoverer Extractor, the NOME macro, developed by LexUm and the University of Montreal and the PIVOINE program of the French technical agency for hospitalization, ATIH).

Notes

- The software referred to above can help in anonymizing documents, but at this time, they require an action on the part of the user (configuration and visual verification).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

2. Addressing the impacts

2.1. Backing up the personal data

Objective: to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality.

Good practices when the measure is selected to treat the risks

- Backup the personal data regularly, whether they are on paper or in electronic form, based on the businesses' availability and integrity requirements.
    - *Recommendations: incremental backup may be performed daily, a complete backup performed weekly and paper documents may be copied when they are written; backups may be verified automatically after that, guaranteeing integrity by producing a report at the end of backup.*
- Implement mechanisms for encrypting the data transmission channel if the network's backup is automated.
- Protect backed-up personal data with the same level of security as that used in operations.
    - *Recommendations: the backed-up data are already encrypted, backups are encrypted or the storage location of the unencrypted backups provides adequate access protection; store the physical backup media (including tapes, cartridges and disks) at another location than the one where the processed data are stored (and store them in a fireproof and waterproof cabinet); protect the transportation of the backup media (including transfer by an authorized agent and in a secure container).*
- Test the backups regularly.
    - *Recommendations: a data sample retrieved may be tested monthly and a full set of data retrieved may be tested annually.*
- Test the integrity of the backed-up personal data if the businesses' requirements so require.
    - *Recommendations: the SHA-256 function is used to take a fingerprint of the backed-up personal data or an electronic signature.*
- Formalize the level of commitment of the IT department regarding the recovery of encrypted information in the event of loss or unavailability of the secrets ensuring the encryption (including passwords and certificates) and regularly check the procedures associated with that commitment.
- Ensure that the organization, employees, systems and premises necessary to carry out the processing are available within a timeframe that corresponds to the needs of the businesses.
- Confirm the geographic location of the backups and, specifically, in which country (countries) the data are stored.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Notes

- Transfers of personal data (and, thus, of backups) to countries outside the European Union are prohibited unless:[39]
  - they involve a transfer to a country that the European Commission recognizes as "adequate;"
  - the issuer and recipient of the data have signed model contract clauses approved by the European Commission;
  - binding corporate rules (BCR) have been adopted (within a group);
  - in the case of a transfer to the U.S., the recipient company has opted into the Safe Harbor program;
  - one of the exceptions set forth in Article 69 of the [Act-I&L] is invoked.

The CNIL website includes a world map indicating the formalities to be followed for each country.[40] In all cases, the data controller remains responsible for the security of the backed-up personal data.

[39] Each of these legal points is addressed in detail on the CNIL site: http://www.cnil.fr/vos-responsabilites/le-transfert-de-donnees-a-letranger/

[40] http://www.cnil.fr/pied-de-page/liens/les-autorites-de-controle-dans-le-monde/

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

2.2. Protecting personal data archives[41]

Objective: to define all procedures for preserving and managing the electronic archives containing the personal data intended to ensure their value (specifically, their legal value) throughout the entire period necessary.

Good practices when the measure is selected to treat the risks

- Confirm that the archive management processes are defined.
  - *Recommendations: distinguish the delivery, storage, management of descriptive data, consultation/communication and administration (relationship with the offices of origin, technological and legal monitoring, upgrade and migration of media and formats).*
- Confirm that the archiving roles are identified.
  - *Recommendations: distinguish the offices of origin, transferring agencies, archiving authorities and inspection agencies (exercising scientific and technical control over the public archives).*
- Confirm that the measures can ensure, if necessary, the identification, authentication, integrity, intelligibility, readability, availability and accessibility of the archives, how long the archives must be kept and the traceability of the operations carried out on the archives (including transfer, consultation, migration and deletion) and take additional measures if they cannot be ensured.
  - *Recommendations: implement access methods specific to the archived data, encrypt the archives and prepare to re-encrypt them securely with new keys before the end of life of the encryption keys; prepare to change obsolete data processing media; choose a procedure ensuring that the entire archive has been destroyed.*
- Determine the methods for protecting the confidentiality of the archived personal data based on the risks identified.
  - *Recommendations: systematically encrypt the sensitive[42] archived personal data.*
- Confirm that the archive authorities have an archiving policy (AP).
  - *Recommendations: the AP document should formalize the legal, functional, operational and technical restrictions that the various actors must comply with so that the electronic archiving established can be considered reliable and permanent.*
- Confirm that a declaration of archiving practices (DAP) exists.
  - *Recommendations: the DAP document should describe all procedures established to achieve the objectives set forth in the archiving policy.*

[41] Archiving methods differ from those used for data in current use and their back-up in that an archive must be used on an occasional, exception basis.
[42] Sensitive data within the meaning of Article 8 and the data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Tools/For further information

- See the [ANSSI-Archivage] and the [NF-42-013] standard.
- See the Archives de France site.[43]

2.3. Monitoring the integrity of personal data

Objective: to be warned in the event of an unwanted modification or disappearance of personal data.

Good practices when the measure is selected to treat the risks

- Identify the data that must be monitored for integrity based on the risks identified.
- Choose a method for monitoring their integrity based on the context, the risks assessed and the robustness required.
  - *Recommendations: use a hash function to generate a fingerprint (hash) of the data to treat the risks related to errors; apply a message authentication code [44] (MAC[45]) to treat the risks related to errors and modification by any person unfamiliar with the key; apply an electronic signature function to treat the risks related to errors and modification by anyone other than the signatory.*
- Determine when the function is to be applied and when the monitoring should be performed based on implementation of the business process.
  - *Recommendations: to monitor the integrity of the data at every use, each piece of data may be fingerprinted when entered, another fingerprint may be taken each time the data are displayed and a visual warning may appear if they do not match (in which case, the data can be restored if they were backed up previously).*

2.3.1 Hash function

Good practices when the measure is selected to treat the risks

- Use a mechanism that is recognized by the appropriate organizations.
  - *Recommendations: use a hash function that complies with the [RGS], such as SHA-256, to calculate a fingerprint of the data and transmit it (via a different channel or after having signed it electronically) so that the integrity of the data is confirmed upon receipt when sent via email, or store it securely so that it can be monitored for integrity when the data are used in the case of safeguarding, archiving or simply storing.*

[43] http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques.
[44] Code that accompanies the data to ensure their integrity by verifying that they have not been changed in any way.
[45] Message Authentication Code.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

2.3.2 Message authentication code

Good practices when the measure is selected to treat the risks

- Choose a mechanism recognized by the appropriate organizations and that provides security proof.
  - *Recommendations: use an algorithm to calculate a message authentication code that complies with the [RGS], such as the "retail" CBC-MAC[46] using the AES as a block encryption mechanism and two separate keys (one for the CBC chain and the other for "retail" superencryption).*

2.3.3 Electronic signature function

Good practices when the measure is selected to treat the risks

- Use only one key for a single purpose.
- Adopt encryption solutions based on public algorithms known to be strong.
  - *Recommendations: use tools (signature creation devices, signature creation application et signature verification module) that are certified, qualified or subject to first-level security certification by ANSSI[47] at the level corresponding to the robustness expected.*
- Choose a mechanism recognized by the appropriate organizations and that provides security proof.
  - *Recommendations: use mechanisms that comply with the [RGS], such as RSA-SSA-PSS[48] or ECDSA[49], using one of the P-256, P-384, P-521, B-283, B-409 or B-571 curves.*
- Generate the keys pursuant to the [RGS].
  - *Recommendations: contract with an electronic certificate service provider[50] that complies with Version 1.0 of the [RGS] for signature use.*
- Establish mechanisms for verifying the electronic certificates.
  - *Recommendations: when an electronic certificate is received, verify, at a minimum, that it includes an indication of purpose consistent with expectations, that it is valid and has not been revoked and that a proper chain of certification exists at all levels.*
- Protect the security of key generation and use consistent with their level in the key hierarchy.
- Formalize the key management system.
  - *Recommendations: develop a "certification policy" (CP) that specifies the responsibilities, identification and authentication, the certificate life-cycle operational requirements, the non-technical and technical security measures,*

[46] *Cipher-block chaining - Message Authentication Code*.
[47] Provided that at least one such reference is included in the catalogue of products that have obtained ANSSI qualification. Otherwise, the PSCE seeking to obtain qualification for its range of authentication certificates must obtain an exemption from the ANSSI.
[48] RSA Signature Scheme with Appendix – Provably Secure encoding method for digital Signatures.
[49] Elliptic Curve Digital Signature Algorithm.
[50] See http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

the certificate and revocation lists profiles, compliance audits and other evaluations.

Tools/For further information

- See the ANSSI's explanations regarding electronic signatures.[51]
- See the [RGS] requirements regarding the "Electronic Signature" function.

Note

- If a smart card is used as a signature creation device, use a smart card reader with a built-in PIN-pad that can enter the activation code and confirm it without transmitting the code via the computer or public access terminal used.

[51] See http://www.ssi.gouv.fr/site_rubrique59.html.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

2.4. Tracing the activity on the IT system

Objective: to allow early detection of incidents involving personal data and to have information that can be used to analyze them or provide proof in connection with investigations.

Good practices when the measure is selected to treat the risks

- Set up a logging architecture that retains a record of security incidents and the time they occurred.
  - *Recommendations: datestamp and timestamp the logged incidents based on UTC time,[52] use a reliable time source (such as an NTP[53] server or radio synchronization) to synchronize the equipment; centralize locally (assemble all the logs on a relatively isolated collection machine supported by a dedicated consultation workstation); export the logs (scheduled dispatches, automatic transfer or an administration network); provide for sufficient storage capacity; set up an archiving and back-up system for the incident logs; protect the logging equipment and the information logged against sabotage and unauthorized access.*
- Select the incidents to be logged based on the context, supporting assets (including workstations, firewall, network equipment and servers), risks and legal framework.
  - *Recommendations: log the actions on the workstations only in the case of heightened risks; comply with the French Postal and Electronic Communications Code if public Internet access[54] is established, with a strict duty of confidentiality; comply with the [Décret-LCEN] if online content is created.[55]*
- Comply with the requirements of the [Act-I&L] if the logged incidents include personal data.
  - *Recommendations: users must be informed of the systems used, those systems' use must be declared to the CNIL and the use of the data collected must comply with the purpose stated initially.*
- Conduct periodic analyses of the logged information and establish a system that detects weak signals automatically.
- Retain the incident logs for six months unless legal and regulatory restrictions require specific retention periods.

[52] Coordinated Universal Time.
[53] Network Time Protocol.
[54] Retain connection data for one year if they are collected in connection with the service, information allowing the user and the recipient(s) of the communication to be identified, data on the communication terminal equipment used, technical features, the date, schedule and duration of each communication and data on the additional services requested or used and their suppliers.
[55] Retain the following for one year if they are collected in connection with the service: connection data, content creation data, contract-related data and payment-related data.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Tools/For further information

- See the [CERTA-Journaux] note.
- Consider implementing the [RGS] "Time and Date Stamp" function, based on the analysis of risks and legal requirements.

2.4.1 Client workstation

Good practices when the measure is selected to treat the risks

- Confirm that the maximum size of the incident logs is adequate and, in particular, that the oldest incidents are not automatically deleted if the maximum size is reached.
- Log application-, security- and system-related incidents.
  - *Recommendations: connections to the system (record the identifier and date and time of the attempt to connect, whether the connection was successful or not, and the date and time of the disconnection); changes to security, privileges, user and group account settings; system incidents (stop and restart of sensitive system processes); access/change to system data; failure while accessing a resource (system file, object, network); performance of sensitive operations; application of security patches, administration and remote control actions, antivirus software logs (activation/deactivation, updates, detection of malicious codes).*
- Export the logs using domain management functionalities or via a client syslog.
- Analyze primarily the connection and disconnection times, the type of protocol used to connect and the type of user who used it, the original IP connection address, successive connection failures and unplanned interruptions of applications or tasks.

2.4.2 Firewall

Good practices when the measure is selected to treat the risks

- Establish a filtering policy that prohibits any direct communication between the internal workstations and the exterior (permit connections only via the firewall) and allow only those flows that are explicitly authorized (firewall blockage of all connections except those identified as necessary).
- Log all successful authorized connections and all rejected efforts to connect.
  - *Recommendations: for each connection, time- and datestamp the logs to the nearest millisecond, log, at a minimum, the source and destination IP addresses, the transport protocol and the flags and connection states associated with the segments for the TCP protocol.*
- Export the logs via a secure channel to a dedicated server.

2.4.3 Network equipment

Good practices when the measure is selected to treat the risks

- Log the activity on each port of a switch or a router.
- Export the logs to a dedicated server using an integrated client syslog or via a netflow.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- Monitor the volume based on times and monitor compliance with any access control lists[56] for the routers.

2.4.4 Server

Good practices when the measure is selected to treat the risks

- Log as much information as possible regarding client requests on the web servers to identify configuration defects and injections of SQL queries.
    - *Recommendations: successful connections, connection methods, queries, volume, distribution by country of query.*
- Log users' activity on the proxy servers.
- Log all queries made to the DNS servers, whether issued by Internet users or internal network clients.
- Log the time- and date-stamped authentication data and the length of each connection on the remote access servers.
- Log the reception and management of messages on the messaging servers.

[56] ACL.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

2.5. Managing personal data violations

Objective: to have an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.

Personal data breach

"Personal data breach: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed…"

(Amendment of [Directive-2002-58] set forth in [Directive-2009-136])

Good practices when the measure is selected to treat the risks

- Define the roles and responsibilities of the stakeholders, as well as procedures for providing feedback and reactions in the event of a personal data breach.
  - *Recommendations: formalize the responsibilities of the "Data Processing and Civil Liberties" contact (privacy officer or equivalent), interactions with the CNIL, the data subjects and establish a crisis response unit in the event of a damaging event.*
- Establish a directory of individuals responsible for managing personal data breaches.
- Develop a response plan in the event of a personal data breach for each heightened risk, update it and test it periodically.
  - *Recommendations: test the plan at least once every two years.*
- Categorize the personal data breaches based on their impact on data subjects' civil liberties and privacy.
  - *Recommendations: an event is a personal data breach without impacts; an incident corresponds to a personal data breach with isolated impacts; a damaging event is a personal data breach with significant, immediate impacts for one or more subjects; a crisis is a personal data breach with significant, more long-term consequences for one or more subjects.*
- Treat the incidents based on their categorization (event, incident, damaging event or crisis).
  - *Recommendations:*
    - *if the breach involves an event, record it and notify the "Data Processing and Civil Liberties" contact (privacy officer or equivalent);*
    - *if it involves an incident, also resolve it and if possible,[57] notify the subjects affected by the breach;*

[57] Notification of a personal data breach is not required if the data controller has demonstrated, to the satisfaction of the competent authority, that the controller has implemented the appropriate technological protection

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- *if it involves a damaging event, also initiate an in-depth analysis;*
- *if it involves a crisis, also initiate an established management plan.*

- Keep an updated record of personal data breaches.
  - *Recommendations: note the context of the personal data breaches, their effects and the measures taken to resolve them.*
- Analyze the possibility of improving the security measures based on the personal data breaches that have occurred.

Notes

- The "Telecoms Package" adopted by the European Parliament in 2009 and transposed into French law in 2011 creates an obligation to notify the CNIL of certain personal data breaches. This obligation could ultimately involve all data controllers, not only "service providers who offer publicly available electronic communications services." These texts define the form of such notifications:
  - notification of the data subjects shall describe, at a minimum, the nature of the personal data breach and the contacts from whom additional information may be obtained and shall recommend measures to mitigate possible negative impacts of the personal data breach;
  - notification of the national authority with jurisdiction (in France, the CNIL) shall also describe the impacts of the personal data breach and the measures proposed or taken to remedy it.
- It is important to be able to gather, preserve and present proof when legal action follows an incident.

Tools/For further information

- See the [CLUSIF-Victime] procedure.
- See the [CERTA-Intrusion] note.
- See the [Directive-2009-136].

measures and that those measures were applied to the data concerned by the breach. Such technological measures shall render the data unintelligble to any person who is not authorized to access the data.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3. Addressing sources of risk

3.1. Avoiding sources of risk

Objective: to prevent avoidable sources of risk (human or non-human) from harming personal data.

Good practices when the measure is selected to treat the risks

- Store dangerous products (including inflammable, combustible, corrosive, explosive, aerosol and wet items) in appropriate storage areas and at a safe distance from the areas where personal data are processed.
- Avoid dangerous geographic areas (flood zones, areas near airports, chemical industry facilities, earthquake zones and volcanic zones).
- Do not store data in a foreign country without guarantees that can ensure an appropriate level of data protection: if the data are to be transferred to a country that the European Commission has recognized as "adequate" (Canada, Switzerland, Argentina, Guernsey, Jersey and the Isle of Man); if model contract clauses approved by the European Commission are signed between two companies or if binding corporate rules (BCR[58]) have been adopted within a group; in the event of a transfer to the U.S., if the recipient company has opted into the Safe Harbor program or if one of the exceptions in Article 69 of the [Act-I&L] is raised. In all cases, the data controller shall remain responsible for the security of stored personal data and must ensure an appropriate level of storage security.

[58] Binding Corporate Rules.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.2. Marking documents that contain personal data

Objective: to generate cautious behavior among individuals with access to documents (paper or electronic) by clearly identifying those that contain personal data.

Good practices when the measure is selected to treat the risks

- Include a visible, explicit reference on each page of the paper or electronic documents that include sensitive personal data.[59]
  - *Recommendations: include the following language in the heading or footer of sample documents used in connection with processing: "This document includes sensitive personal data" or "This document contains personal data that is protected by law."*
- Include a visible, explicit reference in the subject line of emails that include sensitive personal data.
  - *Recommendations: add "[Personal data]."*
- Include a visible, explicit reference in the business applications that provide access to personal data.
  - *Recommendations: include the following in the letterhead or footer of the application: "This application provides access to personal data that are protected by French Law No. 78-17 of 6 January 1978 regarding information technology, files and civil liberties, amended by French Law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data;" display a statement in correspondence that includes attachments with personal data reminding the sender that he or is dealing with personal data that must be sent to the initial intended recipient and destroyed at the end of the established retention period.*

Notes

- Although visible references may attract the attention of individuals with malicious intent, the benefits generally exceed the risks. A reference in emails with file attachments that contain personal data will serve as a reminder to senders and recipients, who will be more cautious in their handling of these documents. In addition, it will be easier to identify marked documents or correspondence in order to destroy them at the end of the retention period.

[59] Sensitive data within the meaning of Article 8 and the data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.3. Managing persons within the organization who have legitimate access

Objective: to reduce the risks associated with persons within the organization (employees, seconded subcontractors, interns and visitors) who have legitimate access to personal data.

Good practices when the measure is selected to treat the risks

- Determine roles and responsibilities in connection with the protection of personal data.
- Determine the consequences for persons with legitimate access to personal data in the event that they fail to comply with the provisions.
- Draw up an IT charter and annex it to the organization's internal regulations.
- Determine the procedure to be followed systematically when an individual with legitimate access to personal data arrives.
    - *Recommendations: assign a workstation, open an IT account, provide physical means of access, assign a user profile.*
- Obtain the commitment of individuals with legitimate access to the personal data that they will comply with the measures.
    - *Recommendations: require the individuals to sign a confidentiality agreement or provide a specific confidentiality clause in the employment contract regarding personal data.*
- Ensure that individuals with legitimate access to personal data are regularly reminded of the civil liberties and privacy risks and of the measures taken to treat that data and the consequences in the event of failure to comply.
    - *Recommendations: organize an annual information session, send regular updates on policies and procedures that are relevant to the individuals' functions and send reminders by email.*
- Provide appropriate training to individuals with legitimate access to personal data on the tools they use in connection with their work.
- Document the operating procedures, update them and make them available to all users concerned (every action on the system, whether it involves administration operations or the use of an application, must be explained in the users' reference documents).
- Determine the procedure to be followed systematically when an individual with legitimate access to personal data leaves or changes assignment.
    - *Recommendations: return the workstation, close or modify the IT account, return the physical means of access, return the materials and documents that include personal data.*

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Tools/For further information

IT Charter Template

1. Review of the rules on the protection of data and sanctions incurred for failure to comply with the law.

2. The scope of application of the charter, which specifically includes:
   - ❑ internal IT department procedures;
   - ❑ authentication methods;
   - ❑ security rules that must be followed, which may include:
     - o notify the internal IT department of any breach or suspected effort to breach an IT account and, in general, of any malfunction;
     - o never entrust an identifier/password to a third party;
     - o do not modify the workstation settings;
     - o do not install, copy, modify or destroy software without authorization;
     - o lock one's computer when leaving one's workstation;
     - o do not access, try to access or delete information that is not relevant to the user's tasks;
     - o define the procedures for copying data on an external medium, specifically by obtaining the prior agreement of the immediate supervisor and by complying with the rules that have been defined in advance.

3. The procedures for using IT and telecommunications tools and equipment that have been provided, such as:
   - ❑ workstations;
   - ❑ mobile devices;
   - ❑ individual storage space;
   - ❑ local network;
   - ❑ Internet;
   - ❑ email; and,
   - ❑ telephone.

4. The administration conditions for the information system and the existence, where appropriate, of:
   - ❑ automatic filtering systems;
   - ❑ automatic traceability systems; and,
   - ❑ workstation management.

5. Responsibilities and sanctions

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Sample confidentiality agreement regarding personal data

I, the undersigned Mr./Ms. _____, performing the duties of _____ at [company name] (hereinafter referred to as "the Company"), in which capacity I have access to personal data, hereby acknowledge the confidentiality of this data.

Consequently, I undertake, pursuant to articles 34 and 35 of the French Law of January 6, 1978 as amended regarding information technology, files and civil liberties, to take every precaution consistent with normal practices and the state of the art in connection with my responsibilities to protect the confidentiality of the information to which I have access and, in particular, to prevent this data from being changed, damaged or communicated to persons who are not expressly authorized to receive this information.

In particular, I undertake:

- ❑ not to use the data to which I may have access for purposes other than those provided for in connection with my responsibilities;
- ❑ to disclose this data only to those persons, whether public or private, natural or legal persons, who are duly authorized, in connection with their duties, to receive them, ;
- ❑ not to make any copies of this data unless such copying is necessary to perform my duties;
- ❑ to take all measures consistent with normal practice and the state of the art in connection with my responsibilities to prevent the improper or fraudulent use of this data;
- ❑ to take all precautions consistent with normal practice and the state of the art to maintain the physical security of this data;
- ❑ to ensure, within the scope of my responsibilities, that only secure communication methods will be used to transfer this data;
- ❑ to ensure, within the scope of my responsibilities, that the rights of information, access and rectification may be exercised;
- ❑ in the event of termination of my duties, to return all data, computer files and information media relative to this data.
- ❑ [other]

This confidentiality agreement, which shall remain in force throughout the duration of my duties, shall remain in effect for an unlimited period after the termination of my duties for any reason where this agreement concerns the use and communication of personal data.

I have been informed that any breach of this agreement will result in disciplinary and criminal actions and sanctions pursuant to legal provisions in force.

Done at [ ] in [ ] copies.

Name:
Signature:

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.4. Monitoring logical access controls

Objective: to limit the risks that unauthorized persons will access personal data electronically.

3.4.1 Managing users' privileges[60] to access personal data

Good practices when the measure is selected to treat the risks

- Manage users' profiles by separating tasks and areas of responsibility (preferably in centralized fashion) to limit access to personal data exclusively to authorized users by applying need-to-know [61] and least-privilege principles.[62]
    - *Recommendations: define one or several user profiles in centralized fashion (with specific privileges for the use of functions and creation, access, modification, transfer and deletion of data) and assign each person one of the defined profiles when the employment contract takes effect or upon changing jobs.*
- Identify every person with legitimate access to personal data (employees, contracting parties and other third parties) by a unique identifier.
- If the use of generic or shared identifiers cannot be avoided, obtain validation from top management and implement methods for tracing the use of this kind of identifier.
    - *Recommendations: fill out an attendance record, complete a register of activities.*
- Limit access to the tools and administration interfaces to authorized persons.
- Limit the use of accounts that provide elevated privileges to operations that require them.
- Limit the use of "administrator" accounts to the IT department and to administration actions that require them.
    - *Recommendations: "administrator" accounts must be limited to administration tasks; administrators must use an account with more limited rights when they perform actions that are more exposed (for example, reading email or checking the Internet).*
- Every account, particularly if it has elevated privileges (for example, an administrator account), must have its own password.
    - *Recommendations: to the extent possible, "administrator" accounts must be individual and require a personal password.*
- Log information connected to the use of privileges.
- Conduct an annual review of privileges to identify and delete unused accounts and to realign the privileges with each user's functions.
- Withdraw the rights of employees, contracting parties and other third parties when they are no longer authorized to access a premises or a resource or when their employment contract ends and adjust the rights in the event of a job transfer. For individuals with a

[60] Rights to create, access, modify, copy, transfer and delete data.
[61] Each user is authorized to access only the resources necessary to carry out his/her responsibilities.
[62] Each user shall access the resources with the minimum level of privileges allowing him/her to perform the actions necessary to fulfill his/her responsibilities.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

temporary account (including interns and service providers), configure an expiration date when the account is established.

3.4.2 Authenticate individuals who want to access personal data

Good practices when the measure is selected to treat the risks

- Choose an authentication method to open sessions that is appropriate to the context, the risk level and the robustness expected.
  - *Recommendations: if the risks are not elevated, a password may be used; however, if the risks are higher, use a one-time password token[63] but change the default activation password or when part of the password is sent by SMS, a card with a PIN code, an electronic certificate or any other form of strong authentication.*
- Prohibit the passwords used from appearing unencrypted in programs, files, scripts, traces or log files or on the screen when they are entered.
- Determine the actions to be taken in the event of a failed authentication.
  - *Recommendations: block the account after six failures to connect, increase the waiting time between two efforts to connect.*
- Log the information related to local access.
- Limit authentication by identifier and passwords to the workstation access control (unlocking only).[64]
- Authenticate the workstation with the remote information system (servers) using cryptographic mechanisms.

Notes

- A strong authentication mechanism requires a minimum of two separate authentication factors from among something known (for example, a password), something tangible (for example, electronic certificate or smart card) and a characteristic specific to the individual (for example, digital fingerprint or another biometric characteristic).
- In a poorly-secured IT environment (for example, shared workstations), provide for a second authentication to access the application that contains the personal data.
- The [Act-I&L] requires that the CNIL issue prior authorization for the use of biometric systems. In general, the CNIL recommends using "traceless" biometrics (outline of the hand, vein network) or recording of fingerprints on a personal device.

Tools/For further information

- See the requirements regarding the [RGS] "Authentication" function.
- See the [CNIL-Empreinte] document regarding fingerprint-based systems.
- Network access control solutions (NAC) are recommended when many users must be managed.

[63] One-time password.
[64] Such a mechanism constitutes an unlocking mechanism, not a true authentication mechanism.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.4.3 Electronic certificate authentication

Good practices when the measure is selected to treat the risks

- Use only one key for a single purpose.[65]
- Use authentication solutions based on public algorithms known to be strong.
  - *Recommendations: use tools (authentication devices, authentication application and authentication verification module) that are certified, qualified or subject to first-level security certification by ANSSI[66] at the level corresponding to the robustness expected.*
- Choose a mechanism recognized by the appropriate organizations and that provides security proof.
  - *Recommendations: use mechanisms that comply with the [RGS], such as RSA-SSA-PSS[67] or ECDSA,[68] using one of the P-256, P-384, B-521, B-283, B-409 or B-571 curves.*
- Generate the keys pursuant to the [RGS].
  - *Recommendations: contract with an electronic certificate service provider[69] that complies with Version 1.0 of the [RGS] for authentication use.*
- Establish mechanisms for verifying the electronic certificates.
  - *Recommendations: when an electronic certificate is received, verify, at a minimum, that it includes an indication of purpose consistent with expectations, that it is valid and has not been revoked and that a proper chain of certification exists at all levels.*
- Protect the security of key generation and use consistent with their level in the key hierarchy.
- Formalize the key management system.
  - *Recommendations: develop a "certification policy" (CP) that specifies responsibilities, identification and authentication, certificate life-cycle operational requirements, non-technical and technical security measures, certificate and revocation lists profiles and compliance audits and other evaluations.*

3.4.4 Manage the credentials

Good practices when the measure is selected to treat the risks

- Adopt a password policy, implement it and monitor it automatically to the extent that applications and resources allow and inform users about it.

[65] Using the same key for more than one purpose (for example, to encrypt with a confidentiality mechanism and to ensure integrity with a different one) causes many errors. However, this not does prohibit differentiating, locally, two keys from a single secret key provided that the diversification mechanism complies with the [RGS].
[66] Provided that at least one such reference is included in the catalogue of products that have obtained ANSSI qualification. Otherwise, the electronic certificate service provider seeking to qualify its range of authentication certificates must obtain an exemption from the ANSSI.
[67] RSA Signature Scheme with Appendix – Provably Secure encoding method for digital Signatures.
[68] Elliptic Curve Digital Signature Algorithm.
[69] See http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- *Recommendations: passwords shall be composed of a minimum of eight characters; must be renewed if there is the least concern that they may have been compromised and, possibly, periodically (every six months or once a year) and must include a minimum of three of the four kinds of characters (capital letters, lower case letters, numerals and special characters); when a password is changed, the last five passwords may not be reused; the same password should not be used for different accesses; passwords should not be related to one's personal information (including name or birth date).*

- Adopt a specific password policy for administrators, implement it and monitor it automatically to the extent that the applications and resources allow and inform administrators of it.
  - *Recommendations: passwords shall be composed of a minimum of 10 characters and must be renewed every three months; shall be composed of at least three of the four kinds of characters (capital letters, lower case letters, numerals and special characters); when a password is changed, the last five passwords may not be reused; never use the same password for different accesses; passwords should not be related to one's personal information (including name or birth date); configure the software so that it never retains passwords; define a maximum number of tries beyond which a warning is issued and authentication is blocked (temporarily or until it is manually unblocked).*
- Allow users to change their passwords.
- Immediately change default passwords after installing an application or a system.
- Create an initial unique random password for each user account, transmit it securely to the user, for example by using two separate channels (paper and others) or a scratch-off field, and require that it be changed when the first connection is made and when the user receives a new password (for example, if the old password is forgotten).
- Store the authentication information (including passwords for accessing information systems and private keys linked to electronic certificates) so that it is accessible only to authorized users.
  - *Recommendations: limit access rights (including reading and writing) to the absolute minimum and encrypt the files in which the passwords are stored.*
- Sequester the credentials used to administer the IT system resources and keep them updated in a safe or locked cabinet.
- If many passwords or secrets (including private keys and certificates) must be used, implement a centralized authentication solution[70] using OTPs[71] or secure vaults.
  - *Recommendations: access control based, at a minimum, on a robust master password; secure storage of passwords ensuring that the protected passwords cannot be recovered without knowing the secret (including encryption and masking; secure display of passwords (masking of passwords in login boxes); resistant to attack (including decryption, brute force and*

[70] Single Sign-On (SSO).
[71] One-Time Password (OTP).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

replay); automatic closure or blockage (including after a certain period of time or during secure standby).

- If an administrator with privileges to the computer system components leaves, deactivate that person's individual accounts and change any administration passwords that he or she may have known (passwords to functional accounts, generic accounts or service accounts used in connection with the administrator's responsibilities).

Notes

- Mnemonic devices may be used to create complex passwords. For example:
  - using only the first letters of the words in a sentence;
  - using an uppercase if the word is a noun (for example, Chief);
  - retaining punctuation marks (for example, .) ;
  - expressing numbers using numerals from 0 to 9 (for example, one ->1).
- *The phrase {*One forewarned Chief Technical Officer is worth two who have not been warned.} *thus corresponds to the password [1fCTOiw2whnbw.].*
- Be sure to delete all biometric authentication data used in the access control systems.

Tools/For further information

- See the [CERTA-MotsDePasse] note.
- See the requirements regarding the [RGS] "Authentication" function.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.5. Managing third parties with legitimate access to personal data

Objective: to reduce the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.

Good practices when the measure is selected to treat the risks

- Identify all third parties who have or could have legitimate access to personal data.
  - *Recommendations: certain categories of employees, seconded employees (service providers), IT maintenance, business partners and authorized third parties.*
- Determine their role in the processing (including IT administrators, subcontractors, recipients, persons responsible for processing data and authorized third parties) based on the actions they will perform.
  - *Recommendations: if using a cloud computing supplier, the supplier is generally a service provider although in some cases, the supplier may be considered to be a data controller.*
- Determine the respective responsibilities based on the risks connected to the personal data.
  - *Recommendations: establish a "RACI matrix;" that is, determine who is responsible for carrying out each action (R=Responsible), who is accountable (A=Accountable), who is consulted (C=Consulted) and who is kept informed (I=Informed).*
- Conduct a specific evaluation of the potential risks on the data subjects' civil liberties and privacy if these persons access the personal data.
- Determine the appropriate form for establishing rights and obligations based on the third parties' legal structure and their geographic location.
  - *Recommendations: a subcontracting agreement, an agreement, an order or binding corporate rules (BCR).*
- Formalize the rules that persons must comply with throughout the lifecycle of the relationship related to the processing or the personal data, based on the person's category and the actions that he or she will perform.
- Determine a procedure to follow for requests by authorized third parties.
  - *Recommendations: ensure that the requests comply with the texts cited, describe the protocol(s) to be followed in responding to requests so as to minimize the resulting risks and authenticate the parties submitting the requests.*

Tools/For further information

- See [CNIL-TransferOutsideEU] and [CNIL-ExternaliserHorsUE] for cases involving the transfer of personal data outside the European Union.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.5.1 Subcontracting

Good practices when the measure is selected to treat the risks

- Formalize the rules regarding confidentiality of personal data entrusted to a third party.
  - *Recommendations: the third party shall not copy any documents or information media that are entrusted to it, with the exception of those necessary to perform the planned service; shall obtain the prior agreement of the data controller for all operations; shall not use the documents and information processed for purposes other than those specified; shall not disclose the documents or information to other persons, whether public or private, natural or legal; shall take all measures necessary to prevent any improper or fraudulent use of the computer files; shall take all security measures (specifically with regard to hardware) to ensure the preservation and integrity of the documents and information processed throughout the duration of the relationship and, when the relationship terminates, to destroy all manual and computerized files storing the information.*
- Take measures to ensure the effectiveness of the subcontractor's data protection guarantees (data encryption based on their sensitivity or, otherwise, procedures in place ensuring that the service provider does not have access to the data entrusted to it; data link encryption using TLS, SSL or the equivalent; guarantees regarding network protection, traceability, authorization and authentication).
  - *Recommendations: conduct security audits, visit the facilities, require certification of the management of security and/or personal data, obtain regular assessments or audit reports.*
- Develop the operational and contractual tools and resources necessary to terminate the relationship with the service provider, specifically in the event of a breach of contract.
- Formalize the conditions for returning the data and destroying it in the event of a breach of contract or the end of the contract.

Notes

- Article 35 of the [Act-I&L] states that " The contract between the processor and the data controller shall specify the obligations incumbent upon the processor as regards the protection of the security and confidentiality of the data and provide that the processor may act only upon the instruction of the data controller. "

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Tools/For further information

Model confidentiality clauses for use with subcontracting

The computer media and documents provided by Company X to Company Y shall remain the property of Company X.

The data contained in these media and documents are covered by the obligation of professional secrecy (Article 226-13 of the French Criminal Code), as are all data to which Y may have access in connection with the performance of this agreement.

Pursuant to Article 34 of the law on information technology as amended, Y undertakes to take all necessary precautions to protect the security of the information and, specifically, to prevent the information from being altered, damaged or communicated to unauthorized persons.

Y undertakes to comply with the following obligations and to ensure that its employees comply with them:

- not to make any copies of the documents and computer media entrusted to it, with the exception of those necessary to provide the service stipulated in the agreement; this shall require the prior approval of the controller of the file;
- not to use the documents and information processed for purposes other than those specified in this agreement;
- not to disclose these documents or this information to other persons, whether private or public, natural or legal;
- to take all measures to prevent the improper or fraudulent use of the computer files in the course of performing the agreement;
- to take all security measures, specifically physical security measures, to ensure the preservation and integrity of the documents and information processed for the duration of this agreement;
- and, at the end of the agreement, to destroy all manual and computerized files storing the information.

As such, Y may not subcontract the performance of the services to another company or assign the agreement without the prior approval of X.

X reserves the right to conduct any verification it deems appropriate to ensure that Y complies with the obligations mentioned above.

If Y fails to comply with the provisions mentioned above, the holder may also be liable under the provisions of articles 226-5 and 226-17 of the French New Criminal Code.

X may terminate the agreement immediately, without indemnifying the holder, in the event of a breach of professional secrecy or failure to comply with the provisions mentioned above.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.5.2 Outsourcing

Good practices when the measure is selected to treat the risks

- Analyze the risks to assess the issues involved in outsourcing and confirm whether it would be preferable to reduce the scope and, even, not to outsource.
- Stipulate, by contract, the rules on outsourcing all or part of the information system.
    - *Recommendations: formalize the rules regarding the location of the data, transfer of the data to initialize the service, confidentiality, securing the network, access to the services and means of access, management of the identifiers, service availability and continuity, supplier maintenance conditions, management of upgrades and corrective security maintenance, data processing, audits and intrusive testing, data ownership, insurance, reversibility, management of cascade subcontracting, governance and monitoring of the contractual relationship and the prohibition against reducing the security level for economic reasons.*

Notes

- The use of services that offer cloud computing functions requires guarantees with regard to the geographic location of the data (France, within the European Union or outside the European Union).

Tools/For further information

- See the [CNIL-ExternaliserHorsUE].
- See the [ANSSI-Externalisation] guide.

3.5.3 Shared hosting

Good practices when the measure is selected to treat the risks

- Analyze the risks to assess the issues involved in co-hosting and determine whether a dedicated platform, managed by the organization, would be preferable.
- Stipulate, by contract, the rules for accessing the event logs (either in the event of an incident or to monitor the hosted resources).
    - *Recommendations: be able to access the event logs during the business day or monitor incidents in real time; obtain a confidentiality guarantee regarding the logs; obtain certification from the hosting service that all information in the logs are usable given the state of the art.*
- Stipulate, by contract, the rules for monitoring the co-hosted resource.
    - *Recommendations: have indicators on the history of the hosted resource (frequency and monitoring of updates performed, maximum downtime and monitoring of downtime, frequency of backup and data recovery tests performed, server and resource network load and the resource, processor load used by the resource and percentage of the server load, memory load used by the resource and percentage of the server load); be familiar with the origin and content of the co-hosted resources, if possible; host only the*

personal data for a single organization or community of interests on a given server.

- Stipulate, by contract, the rules for managing IT attacks.
  - *Recommendations: identify a technical contact and a decision-making contact within the organization and the hosting service who can be reached 24 hours/day, year-round; obtain a guarantee that information will be provided immediately in the event of attack; define "security incident" and incident reporting procedures.*
- Stipulate, by contract, the incident management rules.
  - *Recommendations: designate the organization responsible for processing the incident, which should be able to exercise total control of the resource environment on the client's behalf for purposes of analysis (including sampling of all information necessary to conduct an analysis pursuant to best practices and analysis of the system in operation); manage the incident and carry out post-incident actions (restart, stop, restore a backup; physically isolate a machine from the rest of the network, establish a security perimeter, resource downtime, server downtime and potential penalties, monitor the filtering rules).*
- Stipulate the reversibility rules by contract.
  - *Recommendations: a reversibility clause, which can be activated primarily for security reasons (change in the service provider's shareholders, offshoring of hosting sites), should enable the organization to recover management of its resources; the service provider must provide its assistance throughout the migration period, guarantee the security of the data and applications entrusted to it during their transfer and return or make available all information corresponding to an extract from the former hosting environment (including remote event logs and backups) over a period to be determined.*

Notes

- With regard to health data, hosting services must obtain prior approval from the Minister of Health. Information on filing a request is available at http://esante.gouv.fr/.

Tools/For further information

- See the [CERTA-Mutualisé] note.

3.5.4 Maintenance

Good practices when the measure is selected to treat the risks

- Encrypt or erase the personal data securely before sending any IT resources for external maintenance (including a server, client workstation or network equipment).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- If the personal data cannot be encrypted or erased completely (for example, in the case of a broken hard disk or malfunction) and if the personal data are not sensitive,[72] have the maintenance service provider sign a confidentiality agreement or arrange for the provider to make the repairs on site in the presence of a member of the IT department.
- In the case of sensitive personal data,[73] do not permit the resources to be sent for external repairs, have the repairs done on site in the presence of a member of the IT department and record the actions in a register.
- When maintenance is performed on site, record the work in a register, have a manager from the organization supervise the activity and configure the systems to ensure that remote maintenance is not possible.

Model confidentiality clauses
for use in connection with third-party maintenance

A description shall be prepared for every maintenance operation and shall specify the dates, nature of the operations and names of the persons involved and shall be transmitted to X.

In the case of remote maintenance that enables Y to access X's files remotely, Y shall take all measures to allow X to identify the source of every external intervention. To that end, Y undertakes to obtain prior approval from X before every remote maintenance operation to be performed at its initiative.

Registries shall be maintained under the respective responsibility of X and Y that note the dates and detailed nature of the remote maintenance operations, as well as the names of their authors.

3.5.5 Remote maintenance

Good practices when the measure is selected to treat the risks

- Have the external third party sign a confidentiality agreement.
- Establish robust, specific passwords that are renewed regularly.
- Activate remote dial-in access for remote maintenance only upon request, with dial-in access inactive by default.
- Encrypt the communications channel (for example, SSH or the equivalent).
- Keep a log of remote maintenance access.
- Prevent bouncing from remote maintenance access to the rest of the local network and, more broadly, to wide area networks (WAN).

[72] Sensitive data within the meaning of Article 8 and the data under Article 9.
[73] Sensitive data within the meaning of Article 8 and the data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.6. Combating malicious codes

Objective: to protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of personal data.

Good practices when the measure is selected to treat the risks

- Install an antivirus application on servers and workstations and configure it.
  - *Recommendations: ensure real-time analysis of the system pursuant to the rules defined by the IT department; prevent the user from deactivating the antivirus application at his/her workstation or modifying its parameters; conduct a full, automatic analysis of local disks at least weekly with minimum service disturbance (for example, during off-peak hours or by limiting the system load allocated to the analysis or during non-working hours[74]).*
- Update the antivirus software.
  - *Recommendations: automatically and regularly deploy updates of the antivirus databases and antivirus engines on the servers and workstations and perform emergency updates.*
- Implement filtering measures that can filter network inflows and outflows (including firewalls and proxies).
- Transfer antivirus security events to a centralized server for statistical analysis and *ex post* management of problems (to detect an infected server or a virus that has been detected and not eradicated by the antivirus application).
- Install an anti-spyware program on the workstations, configure it and update it.

Tools/For further information

- See the [CERTA-Virus] note.

[74] In compliance with the rules related to sustainable development and specifically concerning turning computers off.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.7. Controlling physical access

Objective: to limit the risks that unauthorized persons will gain physical access to personal data.

Good practices when the measure is selected to treat the risks

- Categorize areas of the buildings by on risk.
  - *Recommendations: delimit an area open to the public when the organization has a functional duty to greet the public (reception counter, waiting room or meeting room), an area assigned to the service (a controlled-access area corresponding to the offices where personal data are processed) and a security area (housing the servers, network administration stations, the network's active components or sensitive resources such as energy supply and distribution equipment or network and telephony equipment).*
- Maintain an up-to-date list of individuals (including visitors, employees, authorized employees, trainees and service providers) who are authorized to enter each area.
  - *Recommendations: review access rights to the security areas regularly and delete them if necessary.*
- Select methods for authenticating employees that are proportional to the risks associated with each area.
  - *Recommendations: if the risks are low, one person stationed at the reception area is sufficient to identify employees; if they are higher (restricted or security area), an access gate or other form of access control with a proximity badge with the bearer's identification photograph and/or employee identification number is recommended; the badge should be visible.*
- Select visitor authentication methods (for example, persons coming to attend a meeting, external service providers or auditors) proportional to the risks associated with each area.
  - *Recommendations: if the risks are low, authentication may not be necessary; however, if they are high, establish a reception policy for outside visitors based on a predefined schedule, confirm their identification and provide a badge that is valid only for the length of their visit.*
- Define actions to take if authentication fails (identify cannot be confirmed or lack of authorization to enter a security area).
  - *Recommendations: deny entry to the visitor and notify the person in charge of security.*
- Keep a record of access granted after notifying the data subjects.
  - *Recommendations: record visitors' identity, date and time of arrival and departure, maintain an access log dating back up to three months.*
- Visitors with business beyond the public reception areas[75] should be escorted by a member of the organization.
- Protect the most sensitive areas in proportion to the risks.

[75] From the time they arrive, during their visit and until they exit the premises.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- *Recommendations: install a locked door, digital code or videophone; renew the means of access on a regular basis (door entry codes); identify the area with clear, visible signage understandable by all visitors; secure the openings (window bars for ground floor and lower floor premises or reinforced doors with an access control system).*

- Install a warning system in the event of unauthorized entry.
  - *Recommendations: install systems that detect openings and unauthorized entries and that transmit a centralized warning (on-site security and outsourced services), particularly in security areas, and monitor the most sensitive areas using a CCTV system.*

Tools/For further information

- Establish a system to slow individuals who may have penetrated an area they are prohibited from entering and a system for intervening in such situations to ensure intervention before the unauthorized persons can leave the area.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

3.8. Protecting against non-human sources of risks

Objective: to reduce or avoid risks associated with non-human sources (including computer viruses, climate events, fire, water damage, internal or external accidents and animals) that could affect the security of the personal data.

Good practices when the measure is selected to treat the risks

- Establish fire prevention, detection and protection systems.
  - *Recommendations: organize the premises (remove boxes, unused supplies and flammable substances); install an adequate number of fire extinguishers appropriate to various kinds of fire (powder, liquid and gas extinguishers), smoke detectors with alarms and heat detectors with alarms that are transmitted on a centralized basis (on-site security and outsourced services) and extinction by inert gas or air extraction in the IT rooms.*
- Install temperature monitoring systems.
  - *Recommendations: equip the premises with air-conditioning systems with alarms (in the event that the temperature threshold is exceeded) that are transmitted on a centralized basis.*
- Establish a power supply monitoring and relief system.
  - *Recommendations: protect the computer and telephone equipment from power fluctuations and cut-offs via a generator or inverters that manage normal shutdown and continuous operation, with alarms (in the event of cut-off), and that transmit warnings on a centralized basis.*
- Install systems to prevent water damage.
  - *Recommendations: raise the IT and telephony equipment at least 15 cm from the ground in the IT rooms on the ground floor, distance them from water facilities that could break (plumbing, air conditioner and radiator).*
- Ensure that the essential services (including power, water and air conditioning) are sized appropriately based on the systems they support.
- Specify an appropriate response time in the event of failure in maintenance contracts covering the equipment used in the operation of essential and security services (including extinguishers, air conditioners, water, smoke and heat detectors, opening and unauthorized entry detection and generator) and check the equipment at least annually.
- In the case of high availability requirements, connect the telecommunications infrastructure via at least two different, independent access points and ensure that they can switch from one to the other very quickly. If availability needs are very high, consider a back-up site.

Tools/For further information

- See the reference documents published by the Centre national de prévention et de protection (CNPP), the Assemblée plénière des sociétés d'assurances dommage (APSAD) and the *National Fire Protection Association* (NFPA).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4. Protecting supporting assets

4.1. Reducing software vulnerabilities

Objective: to reduce the possibility to expActt software properties (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.) to adversely affect personal data.

Good practices to be followed if the measure is used to treat risks,

- Maintain systems and applications up to data (versions, security patches, etc.) or, where this is not possible (e.g. applications available only on a system that is no longer supported by the software company), isolate the machine and closely monitor the logs.
  - *Recommendations: use versions maintained up to date by the software vendor or a third party; update software automatically by programming automatic daily checks; test updates prior to deploying them throughout the system; make sure that updates can be rolled back in the event they fail; regularly make sure that software licenses are valid, etc.*
- Document configurations and update them whenever major changes are made.
  - *Recommendations: procedures for strengthening IT resources are described; the links required to perform security updates during installation are identified, etc.*
- Reduce the possibilities of function creep.
  - *Recommendations: manage individual access rights according to the principle of least privilege (avoid, in particular, authorizing the use of advanced functionalities where such authorization is not necessary); assign public or private IP addresses where they are actually needed; disable or delete services that are not absolutely necessary; disable or delete unnecessary accounts (guest accounts, default vendor support accounts, etc.); prohibit logical access to remote diagnostic and configuration ports, disable autorun when a removable device is inserted, boot only from the local drive or the local memory, etc.*
- Protect access.
  - *Recommendations: protect the low-level system configuration (e.g. BIOS) with a password, change the default passwords. Block access to the system with a password-protected screensaver that activates after a period of inactivity (5 minutes for maintenance work, no more than 15 minutes for routine use). Display last login dates and times when logging into accounts, etc.*
- Enable protection measures afforded by the system and the applications.
  - *Recommendations: enable logon passwords, the firewall, automatic updates, malware protection, etc., wherever this is allowed by the operating system; enable access controls on applications that feature them, etc.*
- Search for expActtable vulnerabilities, especially on the most critical servers.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- *Recommendations: actively monitor for vulnerabilities found in software used to process data; use vulnerability detection tools (vulnerability scanning software such as Nmap[76] and Nikto[77]) and even intrusion detection and prevention systems (Host Intrusion Prevention); make sure that top vulnerabilities are covered[78], etc.*

- ❑ Protect the integrity, availability and, where necessary, the confidentiality of software and of source codes of internally developed applications, especially if they are rare, innovative or of high market value.
  - *Recommendations: encrypt source codes to reduce the risks of theft; apply a digital signature to protect authenticity and integrity; make backups; store originals and backups in secure locations, etc.*
- ❑ Check system integrity using integrity checkers (which check the integrity of selected files)
  - *Recommendations: continuously monitor changes made to certain files or directories (use software such as Tripwire); check the registry and processes launched by the system (use software such as Spybot); identify the presence of rootkits[79] (use software such as Rootkit Revealer), etc.*

Tools/For further information

- ❑ Depending on the type of application, it may be necessary to ensure the integrity of processing operations by appending signatures to the executable code to guarantee that it has not been altered. In that regard, signature verification during execution (not just prior to execution) makes compromising a program harder.
- ❑ See the following briefing notes: [CERTA-LogicielsObsolètes], [CERTA-iFrame], [CERTA-Injection], [CERTA-Correctifs], [CERTA-Messagerie], [CERTA-CrossSiteScripting] and [CERTA-CrossSiteForgery].

4.1.1 Specific measures for workstations

Good practices to be followed if the measure is used to treat risks,

- ❑ Prohibit local sharing of directories or data on workstations.
- ❑ Store user data on a backed-up network space, not on workstations.
- ❑ If data must be stored on a local workstation, provide users with means of synchronization or backup and inform them how to use these means.
  - *Recommendations: individual spaces on file servers with a detailed file plan; automatic scripts for copying local folders; automatic synchronization tools managed by the IT department, etc.*
- ❑ Prohibit the use of downloaded applications that are not from safe sources.

[76] See http://nmap.org.
[77] See http://www.cirt.net/nikto2.
[78] See http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
[79] Set of techniques and tools for secretly accessing and controlling a computer.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.1.2 Specific measures for cellphones/*smartphones*

Objective: to reduce the risks related to the format, attractiveness and use of cellphones/*smartphones*.

Good practices to be followed if the measure is used to treat risks,

- Configure telephones before delivering them to users.
  - *Recommendations: telephones must automatically lock after a period of inactivity (1 to 5 minutes). The memory card (microSD) on which e-mail is stored must be encrypted. The remote lock must be activated so that the phone's data may be erased in the event of loss or theft. The installation of new applications is restricted (where possible).*
- Inform users, such as in a memo provided at delivery, about how to use their phone, the applications installed on it (e.g. *Business Mail, Exchange, etc.*), the services provided, and the security rules to be followed.
  - *Recommendations: users must not lower the security level of their phone by changing its configuration. They must not open e-mail of unknown origin. They must not store sensitive files (apart from when reading e-mail). They must regularly erase their phone's cache and cookies. They must immediately notify the IT department in the event of an incident. They must not install any software on their phone unless they are expecting to receive such software and it has been sent by a trusted source (check the reputation of the source before installing or using applications or services).*
- Secure the server.
  - *Recommendations: isolate the server from the rest of the network in a specific DMZ or VLAN. Use up-to-date virus, spyware and spam protection. Immediately install operating system security updates. Authenticate devices with digital certificates (where possible), etc.*
- Secure phones at the end of their life cycle.
  - *Recommendations: before disposing of a phone or recycling it. Erase all of its data and settings. Implement a detailed phone dismantlement procedure that includes wiping the phone's memory, etc.*

Tools/For further information

- See the [CNIL-Smartphones] article.
- See the [CLUSIF-Voix] guide.
- See the [ENISA-Smartphone] report.
- More rigorous measures may be taken where risks are considered to be too high: block attachments; trace and analyze traffic with a sensor; verify the effectiveness of encryption; do not store sensitive data[80] locally and do not allow on-line access to sensitive data[81] using a *smartphone* using a non-cached application; do not send

[80] Sensitive data within the meaning of Article 8 and data under Article 9.
[81] Sensitive data within the meaning of Article 8 and data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

sensitive files to *smartphones* by e-mail if there are high risks; use end-to-end SMS encryption software; draw up a whitelist of authorized applications; regularly reinstall a specially made and tested image of the drive, etc.

4.1.3 Specific measures for software acquisitions (purchases, development, etc.)

Good practices to be followed if the measure is used to treat risks,

- Make sure that developers and maintainers have sufficient resources to perform their tasks.
  - *Recommendations: check for clear specifications, suitable documentation, sufficient skills, etc.*
- Favor interoperable and user-friendly applications.
- Carry out IT developments in an IT environment distinct from the running environment.
  - *Recommendations: carry out developments on different computers and in rooms different from those of the running system, etc.*
- Protect the availability, integrity and, where necessary, confidentiality of source codes.
- Impose data entry and recording formats that minimize the amount of data collected.
  - *Recommendations: when collecting an individual's date of birth, the corresponding form field must not make it possible to enter the month and day of birth (use a drop-down menu that limits the choices for form fields), etc.*
- Make sure that data formats are compatible with the implementation of a retention period.
- Integrate access control to data by user categories during development.
- Avoid using free-text fields. If such fields are required, the following wording must either appear as a watermark or disappear once a user starts typing inside the field: "Individuals have a right of access to the information about them entered in this field. The information you enter in this field must be RELEVANT to the context. Such information must neither include any subjective opinions nor reveal 'either directly or indirectly, an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or any information relating to said individual's health or sex life.'"
- Prohibit the use of personal data prior to the release of software; anonymize this data where necessary.
  - *Recommendations: anonymize production data during acceptance testing; securely wipe all devices used to store sensitive data, [82] etc.*
- Make sure that software runs correctly and as specified during acceptance testing.

Tools/For further information

- See the [RGI].

[82] Sensitive data within the meaning of Article 8 and data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.1.4 Specific measures for databases

Good practices to be followed if the measure is used to treat risks,

- Do not use servers used to host databases for other purposes (in particular for browsing websites, accessing e-mail, etc.).
- Unless prohibited by technical constraints, use personal accounts for access to databases.
- Implement measures and/or install systems to safeguard against SQL or script injection attacks.
    - *Recommendations: block the entry of data that is not of a specific type (e.g. by specifying the format). Block the entry of large volumes of data (e.g. by limiting the size of attachments). Make it impossible to use incoming data to perform any tasks (e.g. identify and reject data that may launch an executable command), etc.*
- Set up special measures for sensitive databases[83].
    - *Recommendations: database encryption, encryption of backups, etc.*

4.1.5 Specific measures for Web browsers

Good practices to be followed if the measure is used to treat risks,

- Secure the configuration of Web browsers.
    - *Recommendations: this configuration must include the protection of personal information stored by browsers (forms, passwords, certificates, etc.), the use of a master password in Mozilla Firefox, the impossibility of storing passwords if there are high risks, etc.*
- Deploy a secure browser on all servers and workstations that are to be used to access the Internet or an intranet.
- Limit the number of plugins, remove any that are not used, regularly update those that are left installed.

[83] Sensitive data within the meaning of Article 8 and data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.2. Reducing hardware vulnerabilities

Objective: to reduce the possibility to expActt hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

Good practices to be followed if the measure is used to treat risks,

- Maintain an up-to-date inventory of IT resources used.
    - *Recommendations: maintain the list of workstations and users, locally managed servers, network and telecommunications equipment, and other devices (printers, faxes, etc.). This list should specify information about the equipment, the type of operating system, the network (IP address, MAC address), the main ported applications, the previous versions and the patches installed.*
- Partition off the organization's resources in the event of shared premises.
    - *Recommendations: the LAN used by staff must use dedicated network resources that (i) are placed under the responsibility of the IT department and (ii) are separated from the resources used by other staff on the premises. In the event of shared technical rooms, access to the organization's IT resources must be restricted to the IT department (e.g. dedicated server locked inside a rack).*
- Block access to personal data stored on discarded IT resources.
    - *Recommendations: inspect equipment to make sure that all personal data have been erased from it. Store equipment on site in a secure room until it is taken away. Use a secure erase tool to wipe data from hard disks or built-in memory. If wiping is not possible (due to failure, malfunction, etc.), physically destroy equipment. If equipment disposal is contracted out, have the disposal company sign a confidentiality agreement. Issue an equipment destruction report and retain it for 10 years.*
- Set up physical redundancy of storage units using RAID[84] or an equivalent technology.
- Make sure that the sizes of storage and processing capacities, as well as the conditions of use, are compatible with the intended use of hardware, particularly in terms of location, humidity and temperature.
- Make sure that the power supplies of most-critical hardware are protected from voltage variations and are backed up by a UPS that at least allows such hardware to be shut down normally.
- Protect access to hardware that is sensitive or of high market value.
- Limit the possibilities of hardware alteration.
    - *Recommendations: use security seals to determine whether computers have been opened,* etc.

[84] RAID is a technology that allows data to be distributed across storage devices (such as hard disks) and thus prevent data from being lost if any of the devices fails.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Tools/For further information

- To reduce the risks related to the interception of compromising emanations, emitted either intentionally (e.g. Wi-Fi) or by mishap (electromagnetic interference from hardware), it may be necessary to either divide the premises (see the [ANSSI-ZonageLocaux] directive) and hardware (see the [ANSSI-ZonageEquip] guide) into zones or to use TEMPEST[85] equipment or a Faraday cage in the case of processing operations exposed to very high risks.

4.2.1 Specific measures for workstations

Good practices to be followed if the measure is used to treat risks,

- Ensure that the IT department provides users with workstations that are kept secure and in working order.
- Small workstations, especially laptops, can be easily stolen. They must therefore be equipped with anti-theft cables whenever their users are not nearby and the premises are not protected by physical security measures.
- Retrieve data, except for data defined as private or personal, from workstations before they are assigned to other persons.
- Erase data from workstations before assigning them to other persons or if such workstations are shared.
- Delete temporary data each time a person logs onto a shared workstation.
- If a workstation becomes compromised, inspect the system for all signs of intrusion in order to determine whether other information has been compromised by the attacker.

4.2.2 Specific measures for mobile devices

Objective: to reduce the risks related to the format, attractiveness and use of mobile devices (laptops, PDAs, etc.).

Good practices to be followed if the measure is used to treat risks,

- Encrypt personal data stored on mobile devices.
  - *Recommendations: physically encrypt the entire hard disk. Logically encrypt the entire hard disk via the operating system. Encrypt files individually. Create encrypted containers, etc.*
- Limit the amount of personal data stored on mobile devices to the strict minimum. Prohibit such storage during travel abroad if need be.
- Ensure the availability of personal data stored on mobile devices.
  - *Recommendations: copy personal data to another computer or another server as soon as possible, etc.*
- Erase personal data from mobile devices as soon as such data is entered in the organization's information system.
- Place privacy filters on mobile devices whenever they are used outside the organization.

[85] Transient ElectroMagnetic Pulse Emanations Standard.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- Configure devices so that they lock after a few minutes of inactivity.

Notes

- More and more laptops are equipped with fingerprint readers. The use of such readers is subject to authorization from CNIL unless they are covered under the single authorization [CNIL-AU-027].
- Disk encryption should not be disabled. A copy of the keys should be retained when encryption is available.

Tools/For further information

- See the [ANSSI-Voyageurs] guide for travel abroad.

4.2.3 Specific measures for removable storage devices

Objective: to reduce the risks related to the formats and uses of removable storage devices (USB flash drives, external hard drives, CD-ROMs, DVD-ROMs, etc).

Good practices to be followed if the measure is used to treat risks,

- Limit the use of removable storage devices to those provided by the IT department.
- Prohibit the use of wireless USB flash drives (e.g. Bluetooth)
- Prohibit the use of USB flash drives on hardware that is not secure (no antivirus, firewall, etc.).
- Restrict the use of USB flash drives to work-related purposes.
- Disable the autorun functionality on all workstations (group strategy).
- Encrypt personal data stored on removable storage devices.
- Return removable storage devices that are either defective or no longer necessary to the IT department.
- Securely destroy unnecessary personal data storage devices.
    - *Recommendations: wipe magnetic storage devices with a degausser. Destroy CD-ROMs, DVD-ROMs and other such media with a shredder that has a security level of at least 3 (DIN 32757)*[86].

Tools/For further information

- See the [CERTA-ClésUSB] briefing note.

4.2.4 Specific measures for multifunction printers and copiers

Good practices to be followed if the measure is used to treat risks,

- Change manufacturer default passwords.
- Disable unnecessary network interfaces.
- Disable or delete unnecessary services.
- Encrypt data stored on hard drives wherever possible.
- Restrict the sending of electronic documents to internal e-mail addresses and, in certain cases, restrict the sending of electronic documents to a single e-mail address.

[86] The German DIN 32757 standard defines five shredder security levels based on document sensitivity.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- If maintenance is performed by a third party, set up measures to block access to personal data.
    - *Recommendations: data must be either securely encrypted or erased before hardware is sent out for maintenance. Have the maintenance company sign a confidentiality agreement or have the repairs performed on site in the presence of a member of the IT department where data are sensitive[87] and cannot be completely encrypted or erased (hard drive failure, malfunction, etc.). Prohibit hardware containing sensitive data from being sent out for maintenance, [88]etc.*
- If a locally networked multifunction printer or copier is maintained remotely by a third party, take specific measures to protect access to this equipment.
    - *Recommendations: have the external third party sign a confidentiality agreement. Use individual robust passwords that are changed on a regular basis. Enable dial-in access for remote maintenance purposes only when requested; dial-in access should be disabled by default. Keep a remote maintenance access log. Prohibit the possibility of using remote maintenance to bounce to the rest of the LAN and the Internet, etc.*
- Block access to personal data stored on discarded multifunction printers or copiers.
    - *Recommendations: store equipment on site in a secure room until it is taken away. Use a secure erase tool to wipe data from hard drives or built-in memory. If wiping is not possible (due to failure, malfunction, etc.), physically destroy equipment. If equipment disposal is contracted out, have the disposal company sign a confidentiality agreement. Issue an equipment destruction report and retain it for 10 years.*

[87] Sensitive data within the meaning of Article 8 and data under Article 9.
[88] Sensitive data within the meaning of Article 8 and data under Article 9.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.3. Reducing the vulnerabilities of computer communications networks

Objective: to reduce the possibility to expActt communications networks properties (wired networks, Wi-Fi, radio waves, fiber optics, etc.) to adversely affect personal data.

Good practices to be followed if the measure is used to treat risks,

- Maintain a detailed map of the network up to date.
- Make an inventory of all Internet access points and add them to the network map. Make sure that measures put in place are enforced at each access point.
- Ensure the availability of computer communications networks.
    - *Recommendations: make sure that computer communications networks are able to handle expected traffic flows. Have alternative solutions in the event of a failure, etc.*
- Segment the network into impenetrable logical subnet based on the services intended to be deployed.
    - *Recommendations: partition networks into virtual networks (VLANs) in order to pool together certain kinds of hardware according to logical criteria or by controlling data flows based on network addresses by setting up distinct physical networks in order to separate network traffic between the various groups thus created.*
- Prohibit all direct communication between internal workstations and external networks.
    - *Recommendations: set apart an internal network for which no incoming Internet connections are allowed and a demilitarized zone[89] accessible from the Internet.*
- Only use connections that are explicitly allowed (restrict absolutely necessary communication ports to the proper execution of installed applications) by a firewall[90].
    - *Recommendations: if Web servers can be accessed only via the SSL protocol, allow only incoming IP traffic to port 443 on the computer and block all other communication ports, etc.*
- Monitor network activity after informing data subjects of such monitoring.
    - *Recommendations: set up intrusion detection systems [91] or an intrusion prevention system[92] in order to analyze network traffic in real time and detect any suspicious activity suggestive of a cyber attack scenario.*
- Set up a major intrusion response plan with organizational and technical measures for identifying and containing compromises.

[89] DMZ
[90] -
[91] IDS.
[92] IPS.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- *Recommendations: draw up the necessary crisis management documents (network map, list of staff authorized to work on the system, contact details of administrations or organizations that can provide assistance, etc.).*

- Automatically identify hardware as a means of authenticating connections from specific locations and hardware.
  - *Recommendations: use the unique identifiers of network cards (MAC address[93]) to detect and block connections by unlisted devices.*
- Secure management traffic and restrict or prohibit physical and logical access to remote diagnostic and configuration ports[94].
  - *Recommendations: management tasks on local resources must be based on secure management protocols. Where the use of such protocols is not technically possible, management tasks must be carried out directly on the relevant hardware. Restrict the use of the SNMP protocol, which enables the configuration of network hardware via connection to UDP ports 161 and 162, etc.*
- Prohibit the connection of uncontrolled hardware.
  - *Recommendations: only hardware (computers, PDAs, smartphones, etc.) whose configuration has been expressly approved by the IT department may be connected to or synchronized with the network or workstations.*
- Transmit secret information guaranteeing the confidentiality of personal data (decryption key, password, etc.) in a separate transmission using, where possible, a channel different from that used to transmit data.
  - *Recommendations: send encrypted files by e-mail and provide passwords by telephone or in a text message, etc.*

Tools/For further information

- Network activity may be monitored with the help of:
  - intrusion detection systems (NIDS[95], which monitor networks for security breaches, or HIDS[96], which monitor the security of network-connected computers, or hybrid IDS);
  - intrusion prevention systems (NIPS[97], which monitor entire networks for suspicious traffic by analyzing protocol activity, or WIPS, which monitor wireless networks for suspicious traffic by analyzing wireless networking protocols, or NBA[98], which identifies threats that generate unusual traffic flows, or HIPS[99], which monitor hardware for unusual activity).

[93] Media Access Control.
[94] A physical port is a socket for connecting a cable. A logical port is a number used in communications protocols, especially the TCP protocol used on the Internet.
[95] Network-based Intrusion Detection System.
[96] Host-based Intrusion Detection System.
[97] Network-based Intrusion Prevention.
[98] Network Behavior Analysis.
[99] Host-based Intrusion Prevention.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- See the [CERTA-Filtrage], [CERTA-SSL], [CERTA-Canulars], [CERTA-Spam], [CERTA-Tunnels], [CERTA-Indexation], [CERTA-PHP], [CERTA-IPv6], [CERTA-DNS] and [CERTA-Backscatting] briefing notes.
- See the Authentication function requirements in [RGS].

4.3.1 Specific measures for connections to active network hardware

Good practices to be followed if the measure is used to treat risks,

- Use the SSH[100] protocol or a direct hardware connection for connecting to active network hardware (firewall, routers, switches) and prohibit the use of the Telnet protocol except for direct connections.

4.3.2 Specific measures for remote-administration tools

Good practices to be followed if the measure is used to treat risks,

- Restrict the remote administration of local IT resources to IT department staff and to IT resources within the limits of their duties.
- Uniquely identify users of remote-administration tools.
- Authenticate users of remote-administration tools with at least a robust password and, where possible, a digital certificate.
- Keep a log of the activity of users of remote-administration tools.
- Secure the secure authentication flow.
  - *Recommendations: no clear-text passwords, no replayable sequences, etc.*
- Require users to perform specific actions in order to accept incoming remote-administration connections.
  - *Recommendations: clicking a pop-up.*
- Prohibit changes to the tool's security settings and the viewing of passwords or secret information used.
- Block the retrieval of secret information for the purposes of establishing a connection from a workstation.
- Encrypt all traffic flows.
- Require the tool to inform the user of the end of remote administration or lock the user's session if the user is not at their workstation at the time.

4.3.3 Specific measures for mobile or remote devices

Objective: to reduce the risks related to remotely accessing mobile devices (laptops, PDAs, etc.) or remote devices.

Good practices to be followed if the measure is used to treat risks,

- Where possible, set up a strong solution for authenticating users who access internal information systems.

[100] Secure SHell.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

- *Recommendations: require at least two distinct authentication factors from among something a user knows (e.g. a password, OTP tokens [101] without forgetting to change default activation passwords), something a user has (e.g. a digital certificate, smart card) and something a user is (e.g. a fingerprint, other biometric identifiers), etc.*

- Encrypt communications between mobile devices and internal information systems.
  - *Recommendations: use dedicated private lines. Set up VPN[102] connections using encryption algorithms that are considered to be strong. Use 128-bit SSL encryption for Web services, etc.*
- Install a firewall to protect network traffic to and from mobile devices. This firewall must be enabled as soon as a mobile device leaves the organization's premises.
  - *Recommendations: connect devices to a specific remote-access infrastructure. Prohibit simultaneous connections to both the internal information system and a wireless network. Make it impossible for users to disable the firewall or change its settings, etc.*

4.3.4 Specific measures for wireless interfaces (Wi-Fi, Bluetooth, infrared, 3G, etc.)

Good practices to be followed if the measure is used to treat risks,

- Prohibit non-secure communications for connections via wireless interfaces.
- Prohibit simultaneous network connections via a wireless interface and the Ethernet interface.
- Disable unused wireless connection interfaces (Wi-Fi, *Bluetooth*, infrared, 3G, etc.) on hardware and software.
- Control wireless networks.
  - *Recommendations: only authorize wireless infrastructures that allow staff to access local resources (extension of the LAN) and public Internet access that is completely isolated from the organization's LAN infrastructure. Authenticate users. Encrypt traffic, etc.*

4.3.5 Specific measures for Wi-Fi

Good practices to be followed if the measure is used to treat risks,

- Use the WPA or WPA2 protocol with AES-CCMP encryption or the Enterprise mode of the WPA and WPA2 protocols (using a RADIUS server as well as the EAP-TLS or PEAP subprotocol).
- Prohibit ad-hoc networks.
- Use and configure a firewall at network entry and exit points in order to partition off connected hardware as needed.

[101] One-time password.
[102] Virtual Private Network.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Tools/For further information

- See the [CERTA-Wifi] briefing note.
- MAC address filtering may be used in certain cases to protect Wi-Fi access.

4.3.6 Specific measures for *Bluetooth*

Good practices to be followed if the measure is used to treat risks,

- Impose mutual authentication with remote devices.
- Restrict usage to file sharing with hardware controlled by the IT department.
- Encrypt traffic.

Tools/For further information

- See the [CERTA-Bluetooth] briefing note.

4.3.7 Specific measures for infrared

Good practices to be followed if the measure is used to treat risks,

- Perform authentication prior to establishing connections and sending/receiving files or commands.

4.3.8 Specific measures for mobile telephony networks (2G, 3G and higher, etc.)

Good practices to be followed if the measure is used to treat risks,

- Protect SIM cards with PINs that must be entered each time a device is used.

4.3.9 Specific measures for Web browsing

Good practices to be followed if the measure is used to treat risks,

- Use the SSL protocol (HTTPS) to ensure server authentication and confidentiality of communications.
- Favor keys generated in accordance with [RGS].
  - *Recommendations: use the services of an approved electronic certificate service provider (ECSP)[103] as specified in version 1.0 of [RGS] for server authentication purposes.*

4.3.10 Specific measures for file transfers

Good practices to be followed if the measure is used to treat risks,

- Use the SFTP protocol or possibly the SCP protocol[104].
- Always encrypt files before sending them if the risks are high.

[103] See http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.
[104] Secure CoPy.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.3.11 Specific measures for fax machines

Good practices to be followed if the measure is used to treat risks,

- Place fax machines in a physically secure room only accessible by authorized personnel.
- Set up a personal access code system for the printing of messages.
- When sending faxes, have the identity of the destination fax displayed so that the recipient's identity may be checked.
- Follow up each fax by sending the originals to the recipient.
- Pre-enter the numbers of potential recipients in the fax machine's built-in phone book (where available).

4.3.12 Specific measures for ADSL

Good practices to be followed if the measure is used to treat risks,

- Make an inventory of the local Internet access points.
- Physically isolate the local Internet access points from the internal network.
- Only use them for specific legitimate needs (e.g. loss of availability of access to the direct distance dialing network).
- Enable them only when they are used.
- Disable their wireless interface (Wi-Fi) if they have one.

4.3.13 Specific measures for e-mail

Good practices to be followed if the measure is used to treat risks,

- Encrypt attachments containing personal data.
- Make users aware that they must avoid opening e-mail of unknown origin, and especially risky attachments (with extensions such as .pif, .com, .bat, .exe, .vbs, and .lnk), or configure the system so that it is impossible to open them.
- Make users aware that they should not pass on hoaxes, etc.

4.3.14 Specific measures for instant messaging

Good practices to be followed if the measure is used to treat risks,

- Raise user awareness.
  - *Recommendations: ask users to be careful about what they write, to avoid giving real personal data in forms containing user information, to beware of attachments (do not open files from unknown sources), and to avoid clicking every hyperlink, etc.*
- Prohibit the installation and use of instant messaging software. If such software is necessary, inform users about the risks involved and the good practices to follow.
  - *Recommendations: ask users to only install software that has been downloaded from software vendor sites, etc.*

Tools/For further information

- See the [CERTA-IRC] briefing note.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.4. Reducing the vulnerabilities of individuals

Objective: to reduce the possibility to expActt people (employees, individuals who are not part of an organization but are under its responsibility, etc.) to adversely affects personal data.

Good practices to be followed if the measure is used to treat risks,

- Make sure that individuals who have access to personal data and the processing of such data are qualified for their jobs.
    - *Recommendations: make sure that individuals are properly qualified for their jobs. If they are not, provide training, etc.*
- Make sure that the working conditions of individuals with access to personal data and the processing of such data are satisfactory.
    - *Recommendations: make sure that resources (work capacities and availabilities) are sufficient for assigned tasks, etc.*
- Inform individuals with access to personal data and the processing of such data about the risks of expActtation of their vulnerabilities.
    - *Recommendations: explain to individuals that malicious individuals may take advantage of people who talk too much, are predictable (with routine lives that make repeated spying easy), are easily influenced (naive, gullible, obtuse, low self-esteem, little loyalty, etc.) or are easily manipulated (vulnerable to pressure placed on themselves or their circle of family and friends) in order to adversely affect personal data, etc.*

Tools/For further information

- In some cases, measures should also be implemented to help individuals with access to personal data and the processing of such data transition to changes (new services, new tools, new work methods, etc.).

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.5. Reducing the vulnerabilities of paper documents

Objective: to reduce the possibility to expActt paper documents properties to adversely affect personal data.

Good practices to be followed if the measure is used to treat risks,

- Choose paper products and printing methods that are suitable to the storage conditions (retention period, ambient humidity, etc.).
- Retrieve printed documents containing personal data immediately after they are printed.
- Restrict the distribution of paper documents containing personal data to individuals who require them for work-related purposes.
- Store paper documents containing personal data in a secure cabinet.
    - *Recommendations: store them in a fireproof file cabinet with key lock, a safe, etc.*
- Destroy, using a shredder of the appropriate certification level, paper documents that are no longer necessary and which contain personal data.
    - *Recommendations: destroy paper documents with a shredder that has a security level of at least 3 (DIN 32757[105]).*

Tools/For further information

- In the case of the most-sensitive documents, it is recommended to copy and store them in a different secure location. They may also be protected with tamper-evident security seals.

[105] The German DIN 32757 standard defines five shredder security levels based on document sensitivity.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

4.6. Reducing vulnerabilities related to the circulation of paper documents

Objective: to reduce the possibility to expActt paper document circulation properties (within an organization, delivery by vehicle, mail delivery, etc.) to adversely affect personal data.

Good practices to be followed if the measure is used to treat risks,

- Only send paper documents containing personal data that are necessary for processing.
- Keep close track of the circulation of paper documents containing personal data.
  - *Recommendations: keep a specific record of all documents containing personal information that are sent (list of documents sent, sender's identity and signature, transmission channel, truck driver's/courier's identity and signature, date and time of sending) or received (list of documents received, recipient's identity and signature, date and time of receipt), etc.*
- Choose a transmission channel that is suited to the risks and frequency of transmission.
  - *Recommendations: use the postal service. Use the organization's own services (vehicles and drivers). Use a package delivery company, etc.*
- Improve trust in companies used to deliver paper documents containing personal data.
  - *Recommendations: inform people who deliver paper documents about the risks involved if the documents belong to the organization. Draw up clauses on protecting the availability, integrity and confidentiality of paper documents in agreements with package delivery companies. Verify the identity of truck drivers/couriers, etc.*
- Protect paper documents containing personal data.
  - *Recommendations: send documents by registered mail inside two envelopes. Mark the envelopes as "Confidential". Use envelopes, boxes or other containers that withstand threats from sources other than people (accidents, fires, etc.), etc.*

Tools/For further information

- Where the risks are high, it may also be worthwhile to keep copies of every document distributed, to draw up procedures for dealing with stolen, modified or missing documents, and to protect documents with tamper-evident security seals.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

5. Cross-organizational actions

This chapter describes good practices of privacy protection governance. These practices make it possible to establish general measures for directing and controlling the methods used to protect privacy. They help to treat risks to cross-organizational processing. As they are organizational measures, they may also be used for other processing operations carried out within the organization.

5.1. Managing the organization of the protection of privacy

Objective: to obtain an organization able to manage and control the protection of personal data held within it.

Good practices to be followed if the measure is used to treat risks,

- Have the data controller appoint an assistant to help them enforce the [Act-I&L] and provide such assistant with the means to perform their duties.
    - *Recommendations: appoint a data protection officer (DPO). Set out the DPO's duties in a job description. Provide the DPO with human and financial resources. Allow the DPO to carry out their duties directly alongside the data controller with organizational and decisional freedom and without any conflict of interest. Inform staff-representative bodies of the DPO's role. Organize a consultation with the DPO prior to implementing any further processing operations, etc.*
- Define the roles, responsibilities and interactions between all data protection stakeholders.
    - *Recommendations: define the DPC's duties (maintain the list of processing operations and ensure its accessibility; impartially enforce compliance with the law; report to the data controller, etc.). Separate the roles of the administrator with access to data and the administrator with access to usage tracks. Describe the interactions between the project owners, the ISS manager and the DPC, particularly with regard to all future projects. Define the specific duties related to the management of risks to data protection and privacy. Describe how personal data breaches are treated, etc.*
- Create a monitoring committee formed of the data controller, the person in charge of assisting the controller in enforcing compliance with [Act-I&L] and the stakeholders. This committee must meet regularly (at least once a year) to set objectives and review the organization's entire range of processing operations.

Notes

- Appointing a DPC provides a degree of legal certainty (as the DPC ensures compliance with [Act-I&L]), helps simplify administrative procedures (exemption from the requirement of prior notification of ordinary and routine processing operations), offers personalized access to CNIL's services (extranet, training, personalized follow-up, etc.), demonstrates a commitment to ethic and socially responsible management, and

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

provides a means of capitalizing on informational assets (possibility of assigning, transferring or renting files held by the organization in accordance with [Act-I&L]).

5.2. Managing privacy risks

Objective: to control the risks that processing operations performed by the organization pose on data protection and the privacy of data subjects.

Good practices to be followed if the measure is used to treat risks,

- Map the risks for all the organization's processing operations.
- Update the map periodically and at each major change.
    - *Recommendations: each time a new processing operation is created and at least once a year by a dedicated committee.*

Tools/For further information

- See CNIL's data protection and privacy risk management method.
- See "Adopting a comprehensive approach", "Managing ISS risks", "Aiming for continual improvement", "Systematic commitment: security accreditation" and "Specific tools for different categories of on-line services" in [RGS].
- See the [ANSSI-EBIOS] method.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

5.3. Managing the privacy protection policy

Objective: to obtain a documentary base setting out data protection objectives and rules.

Good practices to be followed if the measure is used to treat risks,

- Set out important aspects relating to data protection within a documentary base making up the data protection policy and in a form suited to each type of content (risks, key principles to be followed, target objectives, rules to be applied, etc.) and each communication target (users, IT department, policymakers, etc.).
    - *Recommendations: requirements documented in a set of specifications. A letter to staff explaining management's commitment to privacy protection. Guidelines for users of computer and communications resources. A procedure for including data protection issues in projects, etc.*
- Distribute the data protection policy to those in charge of enforcing it.
- Allow individuals in charge of enforcing the data protection policy to formally request exceptions in the event of implementation difficulties. Review the impacts of all exception requests on the related risks. Have acceptable exceptions approved by the data controller and amend the data protection policy accordingly.
- Establish a multi-annual action plan and monitor its implementation.
- Allow for exceptions to the data protection policy.
- Anticipate how to take into account difficulties in enforcing the data protection policy.
- Regularly check compliance with the rules of the data protection policy and the implementation of the action plan.
    - *Recommendations: check this compliance at least once a year.*
- Regularly revise the data protection policy.

Tools/For further information

- See "Developing an ISS policy" in [RGS].
- See the [ANSSI-PSSI] guide.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

5.4. Integrating privacy protection in projects

Objective: to integrate the protection of personal data in all new processing operations.

Good practices to be followed if the measure is used to treat risks,

- Use CNIL's risk management approach as soon as a service is devised or an application is designed.
- Favor the use of trusted names in ISS and data protection (procedures, products, management systems, organizations, individuals, etc.).
    - *Recommendations: First-level security certification (FLSC). Qualification (standard, enhanced or high). Certification under French decree No. 2002-535 of April 18, 2002, according to seven increasing levels. Accreditation or guarantee (determining the ability to protect classified defense information or sensitive, non-classified defense information). Certification of the information security management system [ISO-27001]. ISS certification of individuals (CISSP – Certified Information Systems Security Professional[106], CISM – Certified Information Security Manager[107], ISO 27001 Lead Auditor[108], etc.), etc.*
- Favor the use of recognized and proven guidelines.
    - *Recommendations: refer to international standards, guides published by institutions (CNIL, ANSSI, etc.), etc.*
- Carry out CNIL formalities before launching new processing operations.

Tools/For further information

- See "Adapting ISS to the issues at stake", "Using products and providers awarded with security certification", and "Efforts commensurate with ISS stakes" in [RGS].
- See the rules and recommendations on "Acknowledging registration and acknowledging receipt" in [RGS] and the associated appendices.
- See the catalogues of products recognized by ANSSI[109].
- See the [ANSSI-MaturitéSSI] and [ANSSI-GISSIP] guides.

[106] See https://www.isc2.org/cgi-bin/content.cgi?category=97.
[107] See http://www.afai.fr/index.php?m=100.
[108] See http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=50&Itemid=27.
[109] The catalogues are available in French on ANSSI's website:
- Certificates: http://www.ssi.gouv.fr/fr/confiance/certificats.html
- CSPN: http://www.ssi.gouv.fr/fr/confiance/certif-cspn.html
- Qualifications: http://www.ssi.gouv.fr/fr/politique_produit/catalogue/index.html

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

5.4.1 Specific measures for on-line services provided by administrative authorities

Objective: to ensure compliance with [Ordonnance-Téléservices].

Good practices to be followed if the measure is used to treat risks,

- Perform a risk analysis to identify the assets to be protected and the threats to be considered.
- Determine security objectives using availability, confidentiality, integrity and traceability criteria in order to ensure adequate protection from risks.
- Using these objectives, determine the necessary security functions and their levels and comply with the rules set for the previously determined level when these functions are described in [RGS] (digital signature, authentication, encryption, time stamping, and in general any encryption mechanisms and key management processes).
- Use security products and service offers from qualified providers.
- Obtain formal certification by an authority, referred to in this context as "accreditation authority", of security accreditation (whereby the administrative authority holds itself liable) and post this certification on the Internet.
- Adopt practices and tools that are recognized as interoperable, in accordance with [RGI] (rules on exchange protocols to be used, Web services and infrastructure).

Notes

- Compliance with [Ordonnance-Téléservices] entails compliance with the requirements of French decree No. 2010-112 of February 2, 2010, used to enforce Articles 9, 10 and 12 of [Ordonnance-Téléservices] as well as the requirements of French decree No. 2007-284 of March 2, 2007, laying down detailed rules on the establishment, approval, amendment and publication of [RGI].
- If an on-line service requires the use of a user-specific identifier, be it a social security number or otherwise, the use of such identifier by an administration is subject to CNIL's prior opinion on draft secondary legislation in accordance with Article 27 of [Act-I&L].

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

5.5. Supervising privacy protection

Objective: to get a comprehensive and up-to-date view of protection of personal data and compliance with [Act-I&L].

Good practices to be followed if the measure is used to treat risks,

- Regularly inspect personal data processing operations to ensure that they comply with [Act-I&L] as well as the effectiveness and appropriateness of planned measures.
  - *Recommendations: perform checks of the most sensitive processing operations and of operations which are the subject of personal data breaches or complaints. Perform random checks so that all operations are inspected on a regular basis. Have a third party perform occasional audits, particularly of the most sensitive processing operations, etc.*
- Set data protection objectives and define indicators for determining whether these objectives are met.
  - *Recommendations: have a map of personal data processing operations and the associated risks. Give prior notification to the CNIL for all processing operations prior to their implementation, etc.*
- Regularly assess data protection.
  - *Recommendations: present the controller with an annual map of risks to all processing operations, an annual assessment of compliance with the data protection policy, a progress report on planned actions, etc.*

Notes

- CNIL plans to approve data protection audit procedures.
- To find out which prior notifications your organization has given to CNIL, send a fax requesting the "Article 31" list and indicating the SIREN number and address of your organization to + 33 (0)1 53 73 22 00.

Tools/For further information

- See the [ANSSI-TDBSSI] guide.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Appendices

Summary table of measures

Measures	Main corresponding chapters in [ISO-27002]
1. Minimize the amount of personal data	15. Compliance
2. Manage personal data retention periods	15. Compliance
3. Inform the data subjects	15. Compliance
4. Obtain the consent of data subjects	15. Compliance
5. Permit the exercise of the right to object	15. Compliance
6. Permit the exercise of the direct access right	15. Compliance
7. Allow the exercise of the right to correct	15. Compliance
8. Partition personal data	10. Communications and operations management
9. Encrypt personal data	10. Communications and operations management
10. Anonymize personal data	15. Compliance
11. Backup the personal data	10. Communications and operations management
12. Protect personal data archives	10. Communications and operations management
13. Monitor the integrity of personal data	10. Communications and operations management
14. Trace the activity on the IT system	10. Communications and operations management
15. Manage personal data violations	13. Information security incident management 14. Business continuity management
16. Avoid sources of risk	9. Physical and environmental security
17. Mark documents that contain personal data	7. Asset management
18. Manage persons within the organization who have legitimate access	6. Organization of information security 8. Human resources security
19. Monitor logical access controls	11. Access control
20. Manage third parties with legitimate access to personal data	6. Organization of information security
21. Combat malicious codes	10. Communications and operations management
22. Control physical access	9. Physical and environmental security
23. Protect against sources of non-human risks	9. Physical and environmental security
24. Reducing software vulnerabilities	10. Communications and operations management 11. Access control 12. Information systems acquisition, development and maintenance
25. Reducing hardware vulnerabilities	7. Asset management 9. Physical and environmental security 10. Communications and operations management 11. Access control

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Measures	Main corresponding chapters in [ISO-27002]
26. Reducing the vulnerabilities of computer communications networks	10. Communications and operations management 11. Access control
27. Reducing the vulnerabilities of individuals	8. Human resources security
28. Reducing the vulnerabilities of paper documents	7. Asset management
29. Reducing vulnerabilities related to the circulation of paper documents	7. Asset management
30. Managing the organization of the protection of privacy	6. Organization of information security
31. Managing privacy risks	6. Organization of information security
32. Managing the privacy protection policy	5. Security policy
33. Integrating privacy protection in projects	12. Information systems acquisition, development and maintenance
34. Supervising privacy protection	15. Compliance

Acronyms

AFNOR — *Association Française de Normalisation* (French National Organization for Standardization)

ANSSI — *Agence Nationale de la Sécurité des Systèmes d'Information* (French Network and Information Security Agency)

APSAD — *Assemblée Plénière des Sociétés d'Assurances Dommage* (certification awarded by the French National Center for Prevention and Protection, CNPP)

CERTA — *Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques* (French Computer Attack and Emergency Response Team)

DPO — Data Protection Officer

CLUSIF — *Club de la Sécurité de l'Information Français* (French Information Security Club)

CNPP — *Centre National de Prévention et de Protection* (French National Center for Prevention and Protection)

CNIL — *Commission Nationale de l'Informatique et des Libertés* (French Data Protection Authority)

DIN — *Deutsches Institut für Normung* (German Institute for Standardization)

ENISA — European Network and Information Security Agency

G29 — *Groupe de travail article 29 sur la protection des données* (Article

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

	29 Data Protection Working Party)
ISO	International Organization for Standardization
NFPA	National Fire Protection Association
RGI	*Référentiel Général d'Interopérabilité* (General Interoperability Framework)
RGS	*Référentiel Général de Sécurité* (General Security Framework)
SSI	Information Systems Security

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

Bibliographic references

[Act-I&L] Act on information technology, data files and civil liberties (Act No. 78-17 of January 6, 1978)[110].
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20110224

An English translation of the law is available at :

http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

[AFCDP-Anonymisation] *Référentiel AFCDP des dispositifs d'anonymisation*, Association française des correspondants à la protection des données à caractère personnel (AFCDP), 2008.
http://www.afcdp.net/L-AFCDP-publie-un-Referentiel-des

[AFNOR-97-560] FD S 97-560:2000, Informatique de santé – Anonymisation – Glossaire et démarche d'analyse et expression de besoins.
http://www.abs92.com/documents/boite_a_outils/notions_fondamentales/notions_de_stat/2_anomysation.pdf

[ANSSI-Archivage] *Archivage électronique sécurisé – Mémento*, 16 mai 2006, ANSSI.
http://www.ssi.gouv.fr/site_article48.html

[ANSSI-EBIOS] *EBIOS 2010 – Expression of Needs and Identification of Security Objectives – Method of risk management*, 7 April 2010, ANSSI.
http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html

[ANSSI-Effacement] *Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter (Problématique de « l'effacement » des signaux magnétiques)*, n°972-1/SGDN/DCSSI, 17 juillet 2003, ANSSI.
http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf

[ANSSI-Externalisation] *Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information*, décembre 2010, ANSSI.
http://www.ssi.gouv.fr/site_article270.html

[ANSSI-GISSIP] *Guide d'intégration de la sécurité des systèmes d'information dans les projets – GISSIP*, 11 décembre 2006, ANSSI.

[110] Amended by French Act No. 2004-801 of August 6, 2004, on the protection of individuals with regard to the processing of personal data, and by French Act No. 2009-526 of May 12, 2009, on the simplification and clarification of French law and the facilitation of procedures.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

http://www.ssi.gouv.fr/site_article86.html

[ANSSI-MaturitéSSI] *Maturité SSI – Approche méthodologique*, 2 novembre 2007, ANSSI.
http://www.ssi.gouv.fr/site_article85.html

[ANSSI-PSSI] *Guide pour l'élaboration d'une politique de sécurité de système d'information – PSSI – Méthodologie*, 3 mars 2004, ANSSI.
http://www.ssi.gouv.fr/site_article46.html

[ANSSI-TDBSSI] *Élaboration de tableaux de bord SSI – TDBSSI – Méthodologie*, 5 février 2004, ANSSI.
http://www.ssi.gouv.fr/site_article47.html

[ANSSI-Voyageurs] *Passeport de conseils aux voyageurs*, ANSSI, janvier 2010.
http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

[ANSSI-ZonageEquip] *Guide n°430 relatif à l'évaluation des équipements commerciaux au sens du zonage TEMPEST*, Direction centrale de la sécurité des systèmes d'information (DCSSI), 1999.

[ANSSI-ZonageLocaux] *Directive n°495 du 19 septembre 1997 relative au concept de zonage TEMPEST, Protection contre les signaux compromettants.*

[CERTA-Backscatting] *E-mail backscatting, pollution par des rapports de non-livraison de courriels*, Note d'information n°CERTA-2008-INF-004, 19 décembre 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-004.pdf

[CERTA-Bluetooth] *Sécurité des réseaux sans fil Bluetooth*, Note d'information n°CERTA-2007-INF-003, 1er août 2007, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003.pdf

[CERTA-Canulars] *Les canulars par messagerie*, Note d'information n°CERTA-2000-INF-005, 14 juin 2000, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005.pdf

[CERTA-ClésUSB] *Risques associés aux clés USB*, Note d'information n°CERTA-2006-INF-006-004, 11 février 2009, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006.pdf

[CERTA-Correctifs] *Acquisition des correctifs*, Note d'information n°CERTA-2001-INF-004, 4 octobre 2001, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004.pdf

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

[CERTA-CrossSiteForgery] *Les attaques de type « cross-site request forgery »*, Note d'information n°CERTA-2008-INF-003, 17 décembre 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003.pdf

[CERTA-CrossSiteScripting] *Vulnérabilité de type « Cross Site Scripting »*, Note d'information n°CERTA-2002-INF-001-001, 14 septembre 2010, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001.pdf

[CERTA-DNS] *Du bon usage du DNS*, Note d'information n°CERTA-2008-INF-002, 25 juillet 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002.pdf

[CERTA-Filtrage] *Filtrage et pare-feux*, Note d'information n°CERTA-2005-INF-006, 10 janvier 2006, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001.pdf

[CERTA-iFrame] *iFRAME, fonctionnement et protection*, Note d'information n°CERTA-2008-INF-001, 17 juillet 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-001.pdf

[CERTA-Indexation] *Outils d'indexation et de recherche*, Note d'information n°CERTA-2006-INF-009, 21 novembre 2006, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009.pdf

[CERTA-Injection] *Sécurité des applications Web et vulnérabilité de type « injection de données »*, Note d'information n°CERTA-2004-INF-001-001, 3 janvier 2005, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001.pdf

[CERTA-Intrusion] *Les bons réflexes en cas d'intrusion sur un système d'information*, Note d'information n°CERTA-2002-INF-002-003, 7 janvier 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002.pdf

[CERTA-IPv6] *Migration IPv6 : enjeux de sécurité*, Note d'information n°CERTA-2006-INF-004-004, 9 janvier 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004.pdf

[CERTA-IRC] *Usage de la messagerie instantanée ou de l'IRC*, Recommandation n°CERTA-2002-REC-001, 28 mars 2002, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-001.pdf

[CERTA-Journaux] *Gestion des journaux d'événements*, Note d'information n°CERTA-2008-INF-005, 31 décembre 2008, ANSSI.

Important: These good practices are provided for guidance; they must be tailored to the risks to be treated.

http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005.pdf

[CERTA-LogicielsObsolètes] *Les systèmes et logiciels obsolètes*, Note d'information n°CERTA-2005-INF-003-010, 16 juillet 2010, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003.pdf

[CERTA-Messagerie] *Mesures de prévention relatives à la messagerie*, Note d'information n°CERTA-2000-INF-002-001, 27 mars 2009, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002.pdf

[CERTA-MotsDePasse] *Les mots de passe*, Note d'information n°CERTA-2005-INF-001, 12 avril 2007, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001.pdf

[CERTA-Mutualisé] *Bonnes pratiques concernant l'hébergement mutualisé*, Note d'information n°CERTA-2005-INF-005, 19 décembre 2005, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005.pdf

[CERTA-PHP] *Du bon usage de PHP*, Note d'information n°CERTA-2007-INF-002, 20 mars 2007, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002.pdf

[CERTA-Spam] *Limiter l'impact du SPAM*, Note d'information n°CERTA-2005-INF-004, 3 octobre 2005, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004.pdf

[CERTA-SSL] *La bonne utilisation des protocoles SSL/TLS*, Note d'information n°CERTA-2005-REC-001, 1er mars 2005, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001.pdf

[CERTA-Tunnels] *Tunnels et pare-feux : une cohabitation difficile*, Note d'information n°CERTA-2001-INF-003-001, 5 octobre 2005, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003.pdf

[CERTA-Virus] *Rappel sur les virus et chevaux de Troie*, Note d'information n°CERTA-2000-INF-007, 8 novembre 2000, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007.pdf

[CERTA-Wifi] *Sécurité des réseaux sans fil (Wi-Fi)*, Note d'information n°CERTA-2002-REC-002, 21 novembre 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002.pdf

[CLUSIF-Victime] *Vous êtes victime d'une malveillance informatique : à quel service d'État vous adresser en France ?*, Club de la sécurité de

l'information français (CLUSIF).
http://www.clusif.asso.fr/fr/production/cybervictime/

[CLUSIF-Voix] *Moyens de Communication Voix : Présentation et Enjeux de Sécurité*, mars 2010, Club de la sécurité de l'information français (CLUSIF).
http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2010-Communication-Voix-Enjeux-de-Securite.pdf

[CNIL-AU-027] Autorisation unique n° AU-027 - Délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels.
http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/254/

[CNIL-DiffJurisprudence] Délibération de la CNIL n°01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence.
http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/17/

[CNIL-Employeurs] *Guide pour les employeurs et les salariés*, CNIL, 2010.
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_employeurs_salaries.pdf

[CNIL-Empreinte] Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, CNIL, 2007.
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf

[CNIL-ExternaliserHorsUE] Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques, CNIL, 2010.
http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/20100909-externalisation.pdf

[CNIL-Smartphones] Les smartphones en questions, CNIL, 2010.
http://www.cnil.fr/la-cnil/actu-cnil/article/article/les-smartphones-en-questions/

[CNIL-TransferOutsideEU] Standard contractual clauses for the transfer of personal data to third countries– Models adopted by the European Communities

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

	and CNIL. http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/contrats-types-de-la-commission-europeenne/ Similar information are available, in English, at : http://www.cnil.fr/english/topics/data-transfers/
[Décret-2002-637]	Décret n°2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000773559&dateTexte
[Decree-I&L]	Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties amended by Act No 2004-801 of 6 August 2004. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000824352&dateTexte An English translation of the decree is available at : http://www.cnil.fr/fileadmin/documents/en/Decree%202005-1309.pdf
[Décret-LCEN]	Décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id
[Directive-2002-58]	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF
[Directive-2009-136]	Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of

privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF*

[ENISA-Smartphone] *Smartphones: Information security risks, opportunities and recommendations for users*, December 2010, ENISA. http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

[G29-Advertising] *Opinion 2/2010 on online behavioral advertising, Article 29 Data Protection Working Party, June 22, 2010*. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[ISO-25237] ISO/TS 25237:2008, *Health informatics – Pseudonymization*.

[ISO-27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[ISO-27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[ISO-27005] ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*.

[ISO-29100] ISO/IEC 29100 draft standard, *Information technology – Security techniques – Privacy framework*.

[ISO-31000] ISO 31000:2009, *Risk Management – Principles and guidelines*.

[ISO-Guide73] ISO/IEC Guide 73:2009, *Risk Management – Vocabulary*.

[LCEN] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/decrets_application/2004-575.htm

[NF-42-013] NF Z42-013:2009, *Electronic archival storage – Specifications relative to the design and operation of information processing*

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00

systems in view of ensuring the storage and integrity of the recordings stored in these systems.

[Ordonnance-Téléservices] Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232

[RGI] *Référentiel Général d'Interopérabilité* (version 1.0), 12 mai 2009, Direction générale de la modernisation de l'État du ministère du Budget, des comptes publics et de la réforme de l'État.
http://references.modernisation.gouv.fr/sites/default/files/RGI_Version1%200.pdf

[RGS] *Référentiel Général de Sécurité* (version 1.0), 6 mai 2010, ANSSI & Direction générale de la modernisation de l'État du ministère du Budget, des comptes publics et de la réforme de l'État.
http://www.ssi.gouv.fr/site_article38.html

FRENCH REPUBLIC
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tel: 01 53 73 22 22 – Fax: 01 53 73 22 00