

# THE CNIL'S GUIDES



## GUIDE SECURITY OF PERSONAL DATA

Edition 2010

This guide is available on the CNIL's website: <http://www.cnil.fr/english/>





## Table of contents

<b>FOREWORD</b>	<b>Page 1</b>
<b>INTRODUCTION</b>	<b>page 3</b>
<b>TERMS &amp; DEFINITIONS</b>	<b>Page 4</b>
<b>Factsheet n° 1 – WHAT RISKS?</b>	<b>page 5</b>
<b>Factsheet n° 2 – USERS AUTHENTICATION</b>	<b>page 7</b>
<b>Factsheet n° 3 – AUTHORISATION MANAGEMENT &amp; AWARENESS RAISING</b>	<b>page 9</b>
<b>Factsheet n° 4 –WORKSTATION SECURITY</b>	<b>page 12</b>
<b>Factsheet n° 5 – HOW TO SECURE MOBILE DATA PROCESSING?</b>	<b>page 13</b>
<b>Factsheet n° 6 – DATA BACKUPS &amp; BUSINESS CONTINUITY MANAGEMENT</b>	<b>page 14</b>
<b>Factsheet n° 7 – MAINTENANCE</b>	<b>page 15</b>
<b>Factsheet n° 8 – TRACEABILITY AND INCIDENT MANAGEMENT</b>	<b>page 17</b>
<b>Factsheet n° 9 – SECURITY OF PREMISES</b>	<b>page 18</b>
<b>Factsheet n° 10 – SECURITY OF INTERNAL NETWORKS</b>	<b>page 19</b>
<b>Factsheet n° 11 – SECURITY OF SERVERS AND APPLICATIONS</b>	<b>page 21</b>
<b>Factsheet n° 12 – SUBCONTRACTING</b>	<b>page 22</b>
<b>Factsheet n° 13 – ARCHIVING</b>	<b>page 24</b>
<b>Factsheet n° 14 – INFORMATION EXCHANGE WITH OTHER ORGANISATIONS</b>	<b>page 25</b>
<b>Factsheet n° 15 – SOFTWARE DEVELOPMENT</b>	<b>Page 27</b>
<b>Factsheet n° 16 – ANONYMISATION</b>	<b>Page 28</b>
<b>Factsheet n° 17 – ENCRYPTION</b>	<b>Page 29</b>
<b>ACRONYME</b>	<b>Page 32</b>
<b>ANNEXES</b>	<b>Page 33</b>



# Foreword

This English translation of the guide *Sécurité des données personnelles* published in 2010 was motivated by frequent requests received from non French-speaking readers. It is the first guide we translate into English. This is both a clear sign of our significant investment in IT security and of our commitment to advance the protection of personal data in a globalized international environment.

Ever since the birth of Internet, security of personal data has been an issue that has known no borders. Today, this is even more true in a world of extensive externalization and cloud computing, where major cyberattacks make the headlines almost every month.

The European directive on the protection of personal data unambiguously requires all companies to implement adequate security measures if they are established in a member state or otherwise make use of data processing means situated in Europe. Our commission is strongly committed to promote this principle nationally, as well as internationally through increased cooperation with other data protection authorities. As such, this guide should be of interest not only to controllers established in France but more generally, to any entity that directly or indirectly uses IT systems in our country.

In this context, this document represents a significant work to catalogue IT best practices when processing personal data for small to medium-size companies. A collection of about forty security measures are listed, allowing to assess the overall security of the most common personal data processing requirements.

We are confident that this work will help improving the adoption of elementary best practices. We appreciate your feedback and help to improve this guide. Please contact us at [sei@cnil.fr](mailto:sei@cnil.fr).

**Isabelle FALQUE-PIERROTIN**  
**CNIL Chairman**

## **Commission nationale de l'informatique et des libertés (CNIL), the French Data Protection Authority**

The CNIL is an independent administrative authority which is responsible for ensuring compliance with the provisions of the French Data Protection and Freedoms Act. As such, it carries out information, advisory, expertise and technology watch missions.

The CNIL holds specific enforcement powers: it verifies the implementation of data processing files and can also perform on-site inspections.

*Foreword of the french version published in 2010:*

The growing importance of data processing in all the spheres of our society leads to the production, processing and dissemination of an increasing amount of personal data.

The threats weighing on IT systems and information networks include computer fraud, purpose circumvention, fraudulent data collection, data loss, vandalism, and most frequent disasters such as fire or floods.

The Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, hereafter referred as the French Data Protection and Freedoms Act (DPA), requires that organisations implementing data processing or holding data files guarantee their security. Data security should be understood as all "useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties" (Art. 34 of the DPA Act). This security must be considered for all the processes applied to this data, whether it is its creation, its use, its backup, its archiving or destruction and concerns its confidentiality, its integrity, its authenticity and their availability.

This practical guide is intended for any person in charge of data processing as well as for any person with a minimum of computer knowledge (system administrator, developer, information system security manager, end-user ...) who wants to evaluate the security level, which must be afforded to any processing of personal data.

It presents a set of essential recommendations arranged by thematic factsheets concerning the security of personal data.

Each factsheet is structured in three sections:

- basic measures;
- what should be avoided;
- further measures.

The section "further measures" is complementary to the basic measures.

Among all the recommendations, some result from good practices in the area of information systems security, while others result from rules regarding the protection of personal data resulting from specific characteristics of such information.

Naturally, this first "security" practical guide could be improved. Therefore, the reader should not hesitate to contact us and provide us with his/her suggestions on the subject.

Of course, in the eyes of experts, this practical guide will not fully answer their expectations; some will find that it does not go far enough, others that it goes too far. Nevertheless, I hope that it will satisfy most readers. I can already reveal that a more elaborate document is currently in preparation.

**Alex TÜRK**  
**CNIL Chairman**

# Introduction

Securing an IT system requires taking into account all aspects of its management. This security resorts to the respect of good practices and the maintenance of the data-processing tool in a state-of-the-art condition with regard to the attacks to which it can be subjected. However, this security will only be effective if rigor is applied to the delivery (and the withdrawal) of security clearances as well as the processing of some unavoidable incidents.

In order to guarantee that all IT system users only have access to the data they need to know, two elements are necessary:

- providing a unique identifier to each user, in association with authentication means: an **authentication method**;
- applying prior access controls to data for each category of users: an **authorisation management**.

In addition, the protection of data concerning persons requires that such data is:

- "collected and processed in an fair and lawful manner" (Article 6 al. DPA Act)
- "collected for determined, explicit and legitimate purposes and is not later on processed in a way that is incompatible with these purposes" (Article 6 al.2 DPA Act).

These requirements can only be assessed by observing how the IT system is used. Consequently, it is necessary to implement a **logging** facility, i.e. recording each user's actions on the system during a defined period of time.

Moreover, the Data Processing and Freedoms Act lays out that data must be "accurate, complete and updated when necessary" (Article 6 al.4 DPA Act). These obligations require information systems to include mechanisms that guarantee data integrity.

The law also lays out that this data "is preserved in a form allowing the identification of the persons concerned for a period of time which shall not exceed the duration required by the purposes for which it is collected and processed " (Article 6 al.5 DPA Act). Therefore, the systems must include a mechanism for any suppression, archiving, or anonymisation of this data when its retention period expires.

Finally, **risk management** represents an effective way to protect "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" (article 1 of Directive 95/46/EC).

As a reminder, CNIL can perform on-site inspections. Moreover, its sanction committee can issue various degree sanctions, such as a warning, an order, a financial penalty, or an injunction to stop processing. The amount of financial penalties can reach €150,000.00 at for the first failure to comply, and then €300,000.00, or 5% of the turnover net of tax of the last fiscal period, limited to €300,000.00 in the case of a Corporation.

The amount of these sanctions "is proportioned to the gravity of the failures to comply and to the benefits drawn from this failure".

CNIL can also refer any penal offence that it is aware of to the Public Prosecutor.

# Terms & definitions

**Authentication:** “the purpose of authentication is to check the identity that an entity is claiming. Generally authentication is preceded by an identification which allows this entity to be recognized by the system via a previous set of elements given. In short, to identify oneself is to communicate one’s own identity, to authenticate oneself is to provide the proof of one’s identity.” (National Agency for the Security of Information Systems, ANSSI).

**Recipient of the data:** “any authorised person to whom the data are disclosed, other than the data subject, the data controller, the sub-contractor and persons who, due to their functions, are in charge of processing the data” (Article 3 of the DPA Act).

**Personal data:** “any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him/her. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration” (Article 2 of the DPA Act).

**Sensitive data:** “personal data that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or related to their health or sexual life” (Article 8 of the DPA Act).

**Data processing controller:** “unless expressly designated by legislative or regulatory provisions relating to this processing, any person, public authority, department or organisation who determines the purposes and means of the data processing” (Article 3 of the DPA Act).

**Third party:** “any person or entity, public authority, department or any other organisation other than the concerned person, the person in charge of the processing, the subcontractor and the persons who, placed under the direct authority of the person in charge of the processing or the subcontractor, are entitled to process the data” (Directive 95/46/EC).

**Processing:** unless otherwise stated in the present document, “processing” means processing of personal data.

**Personal data processing:** “any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction” (Article 2 of the DPA Act).



Risk management gives to the data controller a means to identify what are the useful precautions to take "with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties " (article 34 of the DPA Act).

The 1995 European Union Directive on the Processing of Personal Data further specifies that the protection of personal data requires to take "appropriate technical and organisational security measures" (Article 17).

Indeed such an approach allows an objective decision-making process and the determination of measures that fit perfectly to its context.

**A risk is a scenario which combines a feared situation (ex: breach of the data processing security and its consequences) and the possibilities that it occurs (ex: threats to the supporting assets). Its level is estimated in terms of gravity (extent and number of impacts) and likelihood (possibility / probability of occurrence).**

### Basic measures

The study of risks has to be formalized in a comprehensive document. Such a study will have to be updated on a regular basis, according to the evolutions of the context and must:

- **Take stock** of files and personal data (ex: *customer files, contracts ...*) and the associated processing, whether they are automated or not, by identifying the supporting assets underlying this processing :
  - hardware (ex: *Human resources management server, CD-ROM ...*);
  - software (ex: *operating system, trade software ...*);
  - communication networks (ex: *fiber optic, WIFI, Internet ...*);
  - paper (ex: *printed document, photocopy ...*).
- **Determine** how the persons' privacy could be impacted by these media.
  1. **For each processing, identify and categorize the impacts on privacy, according to their gravity**, in case of a breach of :
    - confidentiality (ex: *identity theft following the disclosure of the pay slips of all the employees of an organisation*);
    - availability (ex: *non-detection of a medicine interaction, due to the inability to access a patient's electronic medical record*);
    - integrity (ex: *modification of the access logs with the intention of wrongly accusing a person*).
  2. **Study the threats** on each media and **prioritize** them according to their probability of occurrence (likelihood).  
Examples of threats: *theft of a laptop PC, contamination via a malicious code, saturation of communication channels, photocopies of paper documents...*(a complete list of threats is provided in appendix 1).
  3. **Study the risk**; which means to combine each impact with the threats it is related to. Thus prioritize the risks obtained according to their gravity and their likelihood.
- **Implement security measures**  
Determine the security measures in order to reduce, transfer or avoid risks. In this guide the practical factsheets give concrete examples of measures intended to cover the obligations resulting from the Data Processing and Freedoms Act: confidentiality, integrity, data quality, storage, collection of assent....

## What should be avoided

- **Undertake a risk study alone.** Involve the most appropriate actors at each stage (trades, project management, data controller...) in order to sensitize them about the risks, make them responsible for their choices and make them to adopt security measures they selected.
- **Undertake a too detailed study.** It is easy to get lost in an inappropriate level of details. The latter must remain consistent with the extent of the study at hand, the goal of the study and its risk level.
- **Select inappropriate measures.** One must determine necessary and adequate measures to handle the risks. They must be adjusted to the constraints of the study (budgetary, technical ...).

## Further measures

- The study of the risks allows the determination of the security measures to be set up. Therefore, **a budget should be set up** for their implementation.
- **The use of a genuine method** allows to have practical tools available and to improve the exhaustiveness and depth of the risk study. The EBIOS<sup>1</sup> toolbox can be used for such a purpose ([http://www.ssi.gouv.fr/site\\_article173.html](http://www.ssi.gouv.fr/site_article173.html)).
- Depending on the available resources, it can also be useful to provide for:
  - the **training** of the persons in charge of the risk studies;
  - a **security audit** of the information system.

---

1 EBIOS - Expression of Needs and Identification of Security Objectives - is the risk management method published by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), French Network and Information Security Agency. EBIOS is a trade mark of the SGDSN.

The data controller must be able to ensure that each user can only access the data that he/she needs to accomplish his/her mission. To that effect, each user must be provided with **an identifier which is his/her own** and must **authenticate himself/herself** before any use of the data processing resources.

Authentication factors of the persons are grouped in three families depending on:

- something the user knows, for example a password,
- something the user has, for example a smart card,
- something the user is or does, for example a fingerprint or a handwritten signature. As a reminder, the Data Processing and Freedoms Act subordinates the use of biometrics to a CNIL<sup>2</sup> preliminary authorisation.

The authentication of a user is qualified as strong when it calls for a combination of at least two of these factors.

### Basic measures

- Users' identifiers (or logins) must, as far as possible, be different from the default accounts defined by the software publishers. The default accounts must be deactivated. No account should be shared among several users.
- In the case of an authentication of users based on **passwords**, their implementation must comply with the following rules:
  - have **at least 8 characters**;
  - use **different types of characters** (uppercase, lowercase, numbers, special characters). Mnemotechnical tricks allow to create complex passwords, for example by:
    - using only the first letters of the words in a sentence;
    - uppercasing if the word is a name (ex: **Chief**);
    - keeping punctuation marks (ex: **'**);
    - expressing numbers using numbers from 0 to 9 (ex: one → **1**);Example, the sentence: "**one** forewarned **Chief** Technical **Officer** is worth **two** who have **not** been **warned**" corresponds to the password **1fCTOiw2whnbw**;
  - **change** the password **regularly** (every 3 months for example).
- When the **renewal** of a password is required, because it was forgotten by the user, once the password has been re-initialized, he/she must be forced to change it on his/her first connection in order to personalize it.

### What should be avoided

- **Communicate one's own password to others.**
- **Keep one's passwords unencrypted** in a file or in a place which is easily accessible by other persons.
- Use passwords linked to personal information (name, date of birth ...).
- Use the same password for different accesses.
- Configure software applications in such a way that they can record passwords.

<sup>2</sup> Regarding this, consult in particular Factsheet 12 - biometrics in the workplace in the CNIL Guide for the employers and employees [http://www.cnil.fr/fileadmin/documents/La\\_CNIL/publications/CNIL\\_GuideTravail.pdf](http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf)

## Further measures

- Regarding the authentication mechanisms it is recommended to refer to *the rules and recommendations concerning suggested authentication mechanisms* in the B3 appendix of the French General Security Reference Framework<sup>3</sup>.
- When authentication methods based on devices are used, such as smart cards or authentication diagrams implementing cryptographic algorithms, these must follow the rules concerning *the selection and the sizing of cryptographic mechanisms* recommended in the B1 appendix of the French General Security Reference Framework<sup>4</sup>.
- When authentication is achieved by **biometric devices** it is necessary to apply for an authorisation from CNIL. In general, CNIL recommends the use of “traceless” biometrics (hand volume, vein pattern matching ...) or the recording of fingerprints in personal device. Regarding devices **based on fingerprints**, the reader is referred to *the CNIL Communication regarding the implementation of fingerprints-based recognition devices with storage in a database* located at the Internet address <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf> in order to find out what the CNIL doctrine is on this matter.

<sup>3</sup> [http://www.references.modernisation.gouv.fr/sites/default/files/RGS\\_Mecanismes\\_Authentification\\_v1\\_0.pdf](http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_Authentification_v1_0.pdf)

<sup>4</sup> [http://www.references.modernisation.gouv.fr/sites/default/files/RGS\\_Mecanismes\\_cryptographiques\\_v1\\_20.pdf](http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf)

Each user of the system should only be able to access the data which he/she needs for performing his/her mission. In concrete terms, this means that **authorisation levels** must be defined as well as **access control mechanisms** protecting the data.

One also must ensure that the users are aware of the threats in terms of security, as well as what is at stake when dealing with the protection of personal data.

### Basic measures

- **Define the authorisation profiles** in the systems by separating the tasks and the fields of responsibility, in order to restrict access to personal data to the users who are duly authorised.
- **Withdraw the users' authorisations as soon as they are no longer authorised to access a room or a resource**, as well as **at the termination of their employment**.
- Document the operating procedures, keep them up to date and make them available to all the users concerned. In concrete terms, any action on the system, whether they are operations of administration-related or plain use of an application, must be explained in documents to which the users can refer.
- Write an **IT charter** and annex it to **staff regulations**.

IT charter structure:

1. **Reminder of the rules of data protection and of incurred sanctions in case of non-compliance with the law.**
2. Application scope of the charter, which includes in particular:
  - methods of intervention of the internal IT department ;
  - authentication means ;
  - security rules to which one must conform to, which can for example include:
    - o inform the internal IT department about any suspected violation or attempt to violate one's IT user account and generally any dysfunction ;
    - o never entrust one's identifier/password to a third party ;
    - o do not modify the configuration of the workstation ;
    - o do not install, copy, modify, destroy software without authorisation ;
    - o lock one's computer as soon as one leaves one's workstation ;
    - o do not access, try to access, or remove information which does not relate to the tasks performed by the user ;
    - o define procedures allowing copying data on an external medium, in particular by obtaining prior authorisation from the supervisor and by complying with previously defined rules.
3. The procedures for the use of IT equipment and telecommunication resources available to the user such as:
  - the workstation;
  - mobile equipment;
  - individual storage space;
  - the local area network;
  - Internet;
  - electronic messaging;
  - telephone.
4. IT administration conditions, and eventually the existence of:
  - automatic filtering systems;
  - automatic logging systems;
  - workstation management tools.
5. Responsibilities and sanctions incurred in the event of non-compliance with the charter.

## What should be avoided

- **Define administrator accounts that are shared by several persons.**

## Further measures

- Establish, document and review **an access control policy that is proportionate to** the purpose of the data processing.  
The access control policy must include:
  - users' registration and revoking procedures intended to grant and withdraw access to data processing;
  - measures prompting users to respect good security practices during the selection and use of passwords or other authentication mechanisms;
  - measures allowing restricting and controlling the attribution and the use of accesses to data processing.
- **Classify information** in order to specifically indicate if this is a sensitive data. This classification allows denoting the security level to be applied.
- Send policy updates and procedures which are relevant for their occupation to all users on a regular basis.
- Organise training and awareness' raising sessions on information security. Periodic reminders can be set up via electronic messaging.
- Arrange for the signature of **a confidentiality agreement** (Cf. typical clause hereinafter), or include in the employment contracts **a specific confidentiality clause** concerning personal data.

### Sample confidentiality agreement regarding personal data:

I, undersigned, Mr. / Mrs. \_\_\_\_\_, employed as \_\_\_\_\_ within the \_\_\_\_\_ Corporation (hereinafter named as "the Corporation"), being in that capacity involved in access to data of a personal nature, states that I acknowledge the confidentiality of the aforesaid data.

Therefore, I am committing, in accordance with articles 34 and 35 of the Law of January 6, 1978 regarding data processing, files and freedoms, modified in 2004, to taking all precautions in conformity with the uses and the state of the art within the framework of my duties in order to protect the confidentiality of the information to which I have access, and in particular to prevent that it is not modified, damaged or communicated to persons not expressly authorized to receive this information.

In particular, I am committing to:

- not using the data which I am able to access for purposes other than those part of my duties;
- only revealing this data to the duly persons authorized, due to their capacity to receive it, whether they are private, public, physical or moral persons;
- not making any copy of this data excepted when it is necessary for the performance of my duties and responsibilities;
- taking all measures in conformity with the uses and the state of the art within the framework of my duties in order to prevent the devious or fraudulent use of this data;
- taking all precautions in conformity with the uses and the state of the art to preserve the material security of this data;

- making sure, within the limits of my duties, that only secure means of communication will be used to transfer this data;
- making sure, within the limits of my duties, the exercise of the information, access and correction rights of this data;
- in the event of suspension of my functions, to completely returning the data, computer files and any information media related to this data.

This confidentiality commitment, in force throughout the duration of my function, will remain effective, without any time limit after the suspension of my functions, whatever its cause, since this commitment relates to the use and communication of personal data.

I have been informed that any violation of this commitment exposes me in particular to criminal and disciplinary proceedings in accordance with the legal provisions into force.

Issued in \_\_\_\_\_ on \_\_\_\_\_ in \_\_\_\_\_ copies

Name:

Signature:

Name:

Signature:

Workstation security requires from the implementation of measures **to prevent**

- **fraudulent access attempts;**
- **virus execution;**
- **remote control takeover, in particular via Internet.**

Risks of intrusion in information processing systems are significant and can lead to the implantation of viruses or "spyware" programs.

### **Basic measures**

- **Limit the number of failed access attempts** to an account. Depending on the context, this number can vary between three and ten. When the limit is reached, it is preferable to temporarily block the possibility to authenticate to this account until intervention by a system administrator.
- Install "**firewall**" software and limit authorised communication ports to those that are strictly necessary for the proper operation of the applications installed on the workstation.
- Use **antivirus protection programs which are updated on a regular basis.**
- Make provision for **an automatic session locking** procedure in the event of non-utilization of the workstation for a given period of time. For maintenance tasks, it is advisable to end a session after one to five minutes of inactivity. For other less critical operations (access to a business application for example), a fifteen minutes delay should be allowed to guarantee security.
- Make provision **to print**, during account connection startup, **dates and times of the previous connection.**

### **What should be avoided**

- **Using obsolete operating systems** (a regularly updated list is available at the following Internet address <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>).

### **Further measures**

- **Limit** the number of applications requiring administrator level rights for their execution.
- **Limit operating system services** being executed on the workstation to those which are strictly necessary.
- Install without delay **operating systems critical updates** by programming a weekly automatic verification.
- Update applications when critical flaws have been identified and corrected.
- Regarding viruses, refer to the CERTA document available at the following Internet address <http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007/> for more comprehensive recommendations.



The multiplication of laptops, USB keys and smartphones makes it necessary to plan for the possible loss of information resulting from the theft or loss of such equipment.

### **Basic measures**

- Implement encryption measures protecting the storage spaces of mobile computer equipment (laptop, removable storage devices such as USB keys, CD-ROMs, DVD-RWs, etc. ...). Among these measures, one can mention:
  - encryption of the hard drive in its entirety at the hardware level;
  - encryption of the hard drive in its entirety at a software level via the operating system;
  - individual file by file encryption;
  - creation of encrypted containers<sup>5</sup>.

Among the available tools, free software applications such as TrueCrypt<sup>6</sup> ([www.truecrypt.org](http://www.truecrypt.org)) allow the creation of encrypted containers secured by a password.

Many laptop manufacturers sell solutions using an encrypted hard drive: it is a good idea to prefer this equipment and to make sure that encryption is properly enabled by the users.

### **What should be avoided**

- Keeping personal data in mobile equipment during a trip overseas. On this subject, one can consult the recommendations made in the document passport advice to travellers (*Passeport de conseils aux voyageurs*) written by ANSSI and available at the following address: [http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs\\_janvier-2010.pdf](http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf)

### **Further measures**

- When mobile equipment is used for data collection while travelling (ex: PDA, Smartphone's or portable PCs, etc.), it is necessary to secure the data stored therein and to foresee the automated locking of the device if it remains idle for a few minutes. Also plan to purge these devices of the collected data as soon as the latter has been imported into the organisation's information system.
- Laptops are more and more often equipped with a digital fingerprint reader. In France, implementation of such devices is subjected to an authorisation from the CNIL.

<sup>5</sup> By container, one means a special file likely to contain several files.

<sup>6</sup> It is advisable to use version 6.0a, which benefits from a first-level security certification by the ANSSI.

Backup copies of personal data must be made and tested on a regular basis, in accordance with the adopted backup policy. It is also necessary to perform the backup of software used for data processing in order to guarantee its continued existence.

Strengthened security is mandatory for the backup of sensitive data.

It is advisable to foresee business continuity by anticipating equipment breakdowns. Physical protection measures against fire or flood damage must be considered.

### **Basic measures**

#### ▪ **Regarding data backup:**

- Carry out frequent backups to avoid information loss. Depending on the volume of information to be backed up, it might be appropriate to perform incremental backups<sup>7</sup> on a daily basis and complete backups less frequently (weekly or twice a month).
- Plan to store backup media on an external site, in waterproof and fireproof safes.
- Combine one or several of the following solutions to secure the backups by either:
  - encrypting the backups themselves;
  - encrypting data at the source;
  - planning storage at a secure location.
- follow rules in adequacy with the security policy regarding the possible transportation of the backups.

#### ▪ **Regarding business continuity management:**

- Install smoke detectors as well as fire extinguishers. These systems must be inspected annually.
- Regarding floods, computer equipment must not be standing directly on the floor. It must be raised above the floor.
- Regarding equipment:
  - The use of an uninterruptible power supply is recommended for the equipment used for critical processing.
  - It is also advisable to implement storage unit redundancy by using a RAID<sup>8</sup> technology.

### **What should be avoided**

- Keeping backups at the same location as the equipment hosting the data. A major loss occurring at this location would result in a final loss of the data.

### **Further measures**

#### ▪ **Regarding business continuity management:**

- Regarding business continuity, plan to size all utilities, such as power or water supply related to the systems involved and to inspect them on a regular basis in order to eliminate any risk of dysfunction or failure.
- Regarding data processing calling for high availability requirements, consider connecting the telecommunications infrastructure by at least two separate channels.

<sup>7</sup> An incremental backup consists in only storing the modifications made in comparison with a previous backup.

<sup>8</sup> RAID refers to data distribution techniques on several backup media (such as hard drives) in order to prevent data loss following the breakdown of one of the media.

During maintenance and technical interventions, data security must be guaranteed. It is also recommended to erase data from equipment to be discarded.

### Basic measures

- Guarantee that data will not be compromised during a maintenance intervention by implementing one or several of the measures listed below:
  - recording of maintenance interventions in **official register**;
  - supervision by a person in charge of the organisation during the interventions of third parties;
  - configuration of mission-critical systems (servers, network equipment ...) in order to prevent their remote maintenance.

- Inspect any equipment containing storage media before it is discarded or it leaves the perimeter of the organisation to ensure that all sensitive data has indeed been erased in a secure way.

As an example, ANSSI grants first level certifications to software performing this task (<http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/> )

On the subject of discarding equipment, one can mention:

- crushers and shredders for paper or digital media such as CD and DVD;
- degaussers<sup>9</sup> for storage units that use magnetic technology.

These recommendations also apply to leased equipment when it is returned at the end of the contractual period.

- Regarding **remote assistance on client workstations**:
  - Remote administration tools must be configured so as to **get the user's consent** before any intervention on his/her workstation, for example by clicking on an icon or while answering a message being printed on the screen.
  - The user must also be able **to observe if remote assistance is in progress** and when it ends, for example by printing a message on the screen.

### What should be avoided

- Install applications for remote maintenance that are vulnerability-prone (ex: some versions of xVNC, Cf. <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-035/> )

### Further measures

- It is necessary to restrict, or even prohibit physical and logical access to diagnosis and remote configuration ports.  
For example, it is necessary to restrict the use of the SNMP protocol that allows the configuration of the network equipment via a connection to the TCP port 161.
- Recommendations concerning discarded equipment are available in the ANSSI document entitled *technical guide for the confidentiality of information recorded on hard drives to be recycled or exported (Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter)* which is available at the following address: [http://www.circulaires.gouv.fr/pdf/2009/04/cir\\_1166.pdf](http://www.circulaires.gouv.fr/pdf/2009/04/cir_1166.pdf).

<sup>9</sup> A degausser is a device performing the irreversible destruction of confidential data by means of demagnetization.

Sample confidentiality clause which could be used in the case of maintenance by a third party:

Each maintenance action will have to be the subject of a description specifying the dates, nature of operations and names of the intervening parties, transmitted to X.

In the event of remote maintenance allowing remote access to the files of X, Y will make all provisions in order to allow X to identify the source of each external intervention. To that end, Y is committed to obtaining prior consent from X before each remote maintenance operation for which he/she would take the initiative.

Registers will be established under X and Y respective responsibilities, stating the date and detailed nature of the remote maintenance interventions as well as the names of their authors.

In order to be able to **later identify a fraudulent access** to personal data, **the abusive use** of such data or to determine the origin of an incident, it is necessary to record the actions performed on the information processing system. To that end, the person in charge of an information processing system must set up a logging process tailored to the risks associated with his/her system. This process must **record the relevant events, guarantee that these recordings cannot be altered**, and in any case **save these elements for a period of time that is not excessive**.

### Basic measures

- Set up a **logging facility** (i.e. storing events in "log files") to record users' activities, abnormalities and events related to security. These logs must save events over a rolling period that cannot exceed six months (except in the case of a legal obligation, or if the CNIL requests, to keep this information longer).  
As a minimum, the users' accesses should be logged including their identifier, the date and time of their connection as well as the date and time of their disconnection. The time-stamping format must preferably take UTC<sup>10</sup> time as reference.  
In some cases, it can be necessary to also log the detailed actions carried out by the user, such as a reference to the consulted data for example.  
Refer to the CERTA document available at the following web address: <http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005>, for an example of implementation.
- **Inform the users** of the installation of such a system.
- **Protect the logging equipment and the logged information** against sabotage and unauthorised accesses.
- Set up procedures detailing the **monitoring of processing use** and **periodically carry out a review of the logged information**.
- **The data controller must be informed as soon as possible about possible security breaches**.
- In the event of fraudulent access to personal data, the data controller should **notify the people concerned**.

### What should be avoided

- Use information coming from the logging facility for another purpose than guaranteeing the proper use of the information processing system.

### Further measures

- Clocks from the various data processing systems of an organisation or from a security domain must be synchronized, using a previously defined reliable time source.  
When the processing requires the use of network resources, synchronization of time sources can be achieved by using the NTP<sup>11</sup> protocol.
- The data controller must **keep himself/herself informed about the technical vulnerabilities** of the systems and undertake suitable actions to address the associated risks.

<sup>10</sup> Coordinated Universal Time

<sup>11</sup> The NTP protocol (Network Time Protocol) allows synchronizing a computer's clock with a reliable time-stamping source.

In order to effectively protect the premises housing the processing of personal data, make provisions for:

- alarms in order to detect an intrusion within a secure zone;
- measures to slow down the progression of persons who managed to enter the premises;
- ways to end the intrusion.

### **Basic measures**

- Restrict access to rooms or offices likely to house equipment containing data by using **locked doors** or a security booth to access the most critical equipment.
- Install **anti-intrusion alarms** and check them periodically.

### **What should be avoided**

- **Undersize or overlook maintenance of the air-conditioning systems** for the rooms housing IT equipment: a failure of these systems often results in IT equipment halting or even in the opening of the doors of the rooms and, therefore, results in effect to the neutralization of elements contributing to the physical security of the premises.

### **Further measures**

- Secure areas must be protected by controls in order to ensure that only duly authorised personnel is allowed to enter these areas. To that end, the following recommendations should be followed:
  - Regarding the areas in which sensitive data is processed or stored, **authentication devices must be considered**. They can consist of access cards with a personal identification number. A log of accesses that occurred during the last three months at the most must be kept up to date in a secure manner.
  - Inside the limited access areas, **require everyone to wear a visible identification badge**.
  - Visitors (personnel in charge of technical assistance, etc.) must be granted limited access. The date and time of their arrival and departure must be recorded.
  - Review and update on a regular basis access authorisations to the secure areas and revoke them if necessary.

For all network services, network functions and service levels necessary for the proper operation of the network must be identified and only these must be authorised.

### Basic measures

- **Limit network traffic to the bare essentials.** For example, if access to a Web server must only go through the SSL protocol, IP network traffic should only reach this equipment via communication port 443 and all other communication ports should be blocked.  
Refer to the following CERTA documents
  - <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/>, for questions about screening and firewalls;
  - <http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001/>, for SSL implementation.
- Secure access to the information system via mobile data processing equipment such as laptops through the establishment of **VPN** connections based on strong well-known cryptographic algorithms<sup>12</sup> and if possible, the use of a hardware device (smart card, One Time Password token, etc.).
- Resort to encrypting communications with the **SSL** protocol using a 128 bit key when setting up Web services.

### What should be avoided

- Use the telnet protocol for the remote connection to active network equipment (firewall, routers, and switches). Rather, **SSH** or a direct physical access to the equipment must be used.
- Set up Wi-Fi networks. If such equipment must be set up, it is necessary to secure the connections by using the **WPA protocol** and select the AES/CCMP encryption mode.  
For more details regarding access to wireless networks, refer to the measures recommended on the CERTA web site at the following address <http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/>

### Further measures

- Network partitioning allows in particular preventing that the compromise of a workstation leads to the compromise of the entire system. In practice, it is recommended to segment the network into logical sub-networks, according to the services that are supposed to be deployed in them.  
An example of such architecture is shown here below.

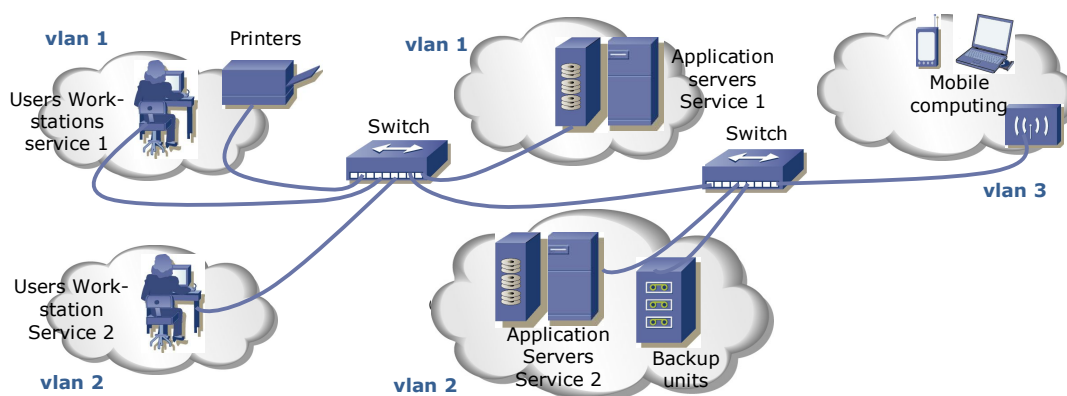


Figure 1: Example of a VLAN partitioned data processing network

12 Cf. Factsheet n°17 – Encryption

In order to implement such a partitioning, several methods can be considered:

- Setting up separate physical networks: it is then possible to partition the various networks by controlling data flows based on network addresses.
- Resorting to virtual networks called VLAN: the goal of this technology is to regroup some equipment connected to a physical equipment (switch) according to logical criteria (for example association to a department), in order to separate network traffic between the various groups thus created.

It is also possible to restrict the authorised connections by, for example, differentiating an internal network for which no connection coming from the Internet is authorised and a network called DMZ (DeMilitarised Zone) accessible from the Internet.

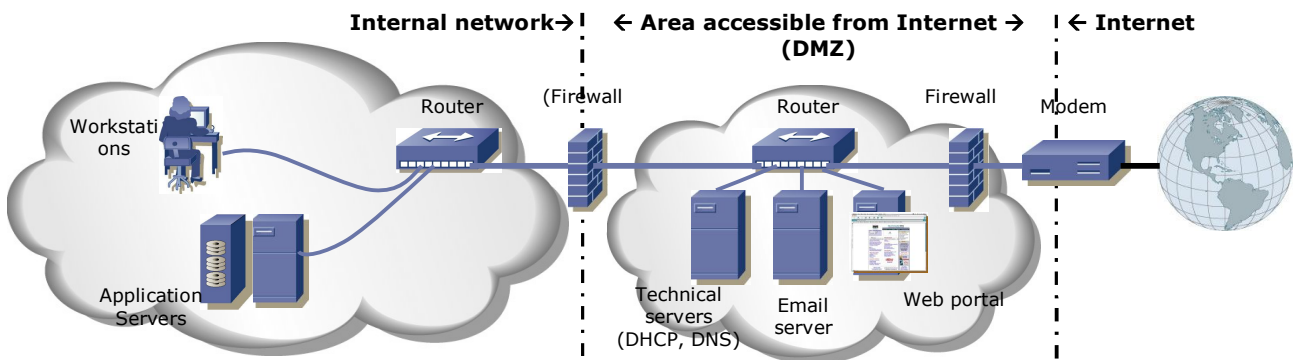


Figure 2: Example of implementation of a DMZ

Implementation of a DMZ calls for the installation of secure bridges (firewalls) between the networks to be partitioned in order to control entering and outgoing information flows.

- Intrusion Detection Systems (or IDS) can be installed in order to analyze real-time network traffic to detect any suspicious activity suggesting a computer attack scenario. The purpose of these systems is to thwart computer attacks as soon as possible. Users of a computer network must be informed if an analysis of the content passing through the network is implemented.
- It is possible to set up automatic equipment identification as a way of authenticating connections from specific locations and equipments. This technique uses for example single identifiers assigned to network cards (MAC address) in order to detect the connection of an unreferenced device and route its network traffic in a separate way.



Servers are the most critical equipment and, thus call for enhanced security measures.

### Basic measures

- Replace default passwords with complex passwords that must at least follow the following rules:
  - must have a **size of at least 10 characters**;
  - must use **different types of characters** (uppercase, lowercase, special numbers and types) ;
  - must be **changed** in particular when **one of the administrators leaves**.
- Install operating systems critical updates without delay by programming a weekly automated verification.
- As far as the administration of databases is concerned:
  - Do not use servers housing databases that are used for other purposes (in particular to browse Internet sites, access electronic messaging ...).
  - Use personalized account identifiers to access databases, except when a technical constraint prevents it to be done.
  - Implement measures and/or install devices to protect against SQL code injection attacks, scripts ...
  - Implement specific measures for "sensitive" databases (database encryption, backup media encryption).
- Ensure business continuity and data availability, which in particular requires taking precautions in the event of software installation or updates on operating systems.
- Update applications when critical flaws have been identified and corrected.

### What should be avoided

- Use unsecured services (cleartext authentication, cleartext flow, etc.).
- Locate databases in an area which is directly accessible from the Internet.

### Further measures

- Sensitive systems, i.e. any system processing sensitive data or data considered as business confidential, must have a **dedicated data processing environment** (isolated).
- When it comes to software being executed on servers, use **vulnerability detection tools** (vulnerability scanners such as nmap (<http://nmap.org/>), nessus (<http://www.nessus.org>), nikto (<http://www.cirt.net/nikto2>) etc.) for the most critical processing, in order to detect potential security flaws. Attack detection and prevention on critical systems / servers called Host Intrusion Prevention can also be used.
- Depending on the nature of the application, it might be necessary to ensure processing integrity by resorting to signatures of the executable code guaranteeing that it was not subjected to any alteration. To this end, a signature verification process carried throughout the execution (and not only before the execution) makes the compromise of a program more difficult.

Personal data communicated to or managed by subcontractors must be processed with security guarantees.

### Basic measures

- In the contracts binding your organisation with subcontractors, consider a specific clause covering the confidentiality of personal data they are entrusted with. A sample clause is provided hereinafter.
- Make provisions (security audits, installations visits, etc.) in order to ensure that the guarantees offered by the subcontractor regarding data protection are effective. That includes in particular:
  - Encrypting data according to its sensitivity, or at least that the subcontractor has procedures guaranteeing it does not have access to the data.
  - Data link encryption (using HTTPS connections for example).
  - Guarantees regarding network protection, traceability (logs, audits), management of security clearances, authentication, etc.
- Envisage the conditions of restitution of data and its destruction in the event of termination or end of the contract.

### What should be avoided

- Resort to services offering cloud computing functions in the absence of any guarantee regarding the **effective geographical location of the data**.

### Further measures

- Concerning health data, health data hosting services must receive an approval issued by the Secretary of Health. The reference framework describing how to request such an approval is available at the following site <http://esante.gouv.fr/>.

Sample confidentiality clause in the case of external processing given to a third party:

**Data-processing media and documents provided by the X Corporation to the Y Corporation remain the property of the X Corporation.**

Data contained in these media and documents is strictly covered by **professional secrecy** (Article 226-13 of the Penal Code); the same applies to all the data that Y comes across of during the execution of the present contract.

In accordance with Article 34 of the French Data Processing Act modified, Y is committed to taking all the necessary precautions in order to preserve the security of information and in particular to prevent that they become garbled, damaged or communicated to unauthorized persons

Therefore, Y commits to respecting the following obligations and making them respected by its personnel:

- not making any copy of the documents and data processing media which are entrusted to it, except for those necessary for the execution of the service envisaged in the contract, prior agreement from the record owner is necessary;

- not using the documents and processed information for purposes other than those specified in the present contract;
- not revealing these documents or information to other persons, whether they are private or public, physical or moral persons;
- taking the necessary measures in order to avoid any devious or fraudulent use of computer files during the execution of the contract;
- taking all security measures, in particular material ones, in order to ensure the preservation and integrity of the documents and information processed throughout the whole duration of the present contract;
- and at the end of the contract, to carry out the destruction of all the manual or computerized files which store the information that was entered.

For this reason, Y will not be able to subcontract the execution of the services to another Corporation, nor carry out a contract transfer of market in the absence of X prior agreement.

X reserves the right to perform any verification which it deems to be useful to observe the respect by Y of the above mentioned commitments.

In the event of non-observance of the above mentioned provisions, the responsibility for the holder can also be committed on the basis of provision of Articles 226-5 and 226-17 of the new Penal Code.

X will be in a position to pronounce the immediate cancellation of the contract, without damages to the benefit of the holder, in the event of breach of professional secrecy or of non-observance of the above mentioned provisions.

One usually distinguishes three types of archives:

- Active databases or current archives: these are current use data used by the departments in charge of the implementation of processing.
- Intermediate archives: this is data that is no longer used but which still presents an administrative interest for the organisation. Data is kept on separate media and is searched in a specific and timely manner.
- Final archives: this is data presenting an historical, scientific or statistical interest which justifies that they are not the object of any destruction. It is governed by the rules contained in book II of the Code of Patrimony and not by the French data protection Act.

Archives must be secured and encrypted if the archived data is sensitive data or considered as business confidential.

### Basic measures

- Implement specific access methods to archived data, due to the fact that the use of an archive is made in a specific and exceptional manner.
- Follow the recommendations given in Factsheet n°17 - Encryption, with regard to the encryption of archives.
- With regard to the destruction of archives, select a procedure guaranteeing that the archive has been destroyed in its entirety.

As an example, ANSSI grants first level certifications to software performing such a task ([http://www.ssi.gouv.fr/site\\_rubrique54.html](http://www.ssi.gouv.fr/site_rubrique54.html))

Depending on the type of media, one can mention:

- Crushers and shredders for paper as well as digital media such as CD and DVD.
- Degaussers for storage units using magnetic technology.

Refer to the document *Technical guide for the confidentiality of information recorded on hard drives to be recycled or exported*. (*Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter* [http://www.circulaires.gouv.fr/pdf/2009/04/cir\\_1166.pdf](http://www.circulaires.gouv.fr/pdf/2009/04/cir_1166.pdf)).

### What should be avoided

- The use of media that do not present adequate guarantees of longevity. As an example, one can mention CDs and DVDs whose longevity seldom exceeds 4 or 5 years.

### Further measures

- Further information on archiving issues is available on the France's archives site: <http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques/>

The **communication** of personal data must be secured, that is to say confidentiality, integrity and authenticity of the information must be ensured.

**Electronic messaging and fax**, even though they save time, **do not generally speaking constitute a secure mean of communication** to transmit personal data. A simple handling error (wrong e-mail, error in dialling the recipient's fax number...) can result in the disclosure of personal information to non-authorized recipients and therefore interfere with the persons' right to privacy.

Moreover, taking into account the general lack of confidentiality of the Internet network, **transmission of personal data via the Internet** presents **significant risks of disclosure of such data** and of intrusion in the internal IT systems.

### Basic measures

- **Regarding the confidentiality of communications:**
  - Encrypt data before it is stored on media when data transmission is carried out by sending a physical media (using optical or magnetic technology).
  - When sending via a network:
    - If such a transmission is done via electronic messaging, encrypt the documents to be transmitted. Regarding this subject, one must refer to the recommendations made in factsheet n° 17 – Encryption.
    - If this is a file transfer, use a protocol guaranteeing confidentiality, such as **SFTP**.
    - If such a transmission uses the HTTP protocol, use the SSL (**HTTPS**) protocol to ensure the servers authentication and the confidentiality of the communications.
- In all cases, **transmission of the secret** (cryptographic key, password, etc.) guaranteeing the confidentiality of the transfer must be carried out through a separate transmission, if possible using a different type of channel from the one used for the transmission of the data (for example: sending of the encrypted file by mail and communicating the password by telephone or SMS).
- If you need to use **a fax**, it is recommended to set up the following measures:
  - The fax machine must be located in a room with physically access controls and only accessible by authorised personnel.
  - Printing messages must be dependent on the introduction of a personal access code.
  - When messages are emitted, the fax must display the identity of the fax recipient in order to ascertain the recipient's identity.
  - Duplicate fax transmission by also sending the original documents to the recipient by mail.
  - Pre-register the potential recipients in the fax machine address book (when this function is available).

### What should be avoided

- **Transmit files containing unencrypted personal data via online web messaging providers** of the Gmail or Hotmail type.

## Further measures

- **Regarding data integrity:**

It is recommended to calculate a fingerprint of the unencrypted data and transmit this fingerprint so that data integrity is verified at reception. Fingerprint calculations can be carried out using hash algorithms such as SHA-1 or SHA-2. Using SHA-2 is recommended.

- **Regarding data authenticity:**

The sender can sign the data before sending it in order to guarantee that he/she is the transmission originator. An electronic signature calls for the setting up of a Public Keys<sup>14</sup> infrastructure (PKI).

Once the various actors have set up a **public keys infrastructure**, the use of public key algorithms seems to be particularly adapted to guarantee the confidentiality and integrity of communications, as well as the sender's authenticity through the use of electronic signatures.

Such an infrastructure consists in delivering a pair of public/private keys to all the persons who potentially exchange information. Public keys must be certified by a certification authority for which each user has the root certificate<sup>14</sup>, so that the authenticity of public keys is guaranteed.

The algorithms implemented within this infrastructure must follow the recommendations of the appendix B1 of the French General Security Reference Framework<sup>15</sup>.

This reference framework specifies in particular the key lengths to be considered. At the time of publication of this document, it is (as an example) recommended that:

- The minimum size of an RSA key shall be 2048 bits, for use not exceeding year 2020.
- For use beyond 2020, the minimum size of the RSA key shall be 4096 bits.

These values are given as an indication; they are dependent on the context specific to each processing.

- After data is received, with its integrity verified by the recipient, and once it has been integrated into the information system, it is recommended to destroy the media or files that were used for its transmission.

14 A certificate is made up of:

1. A public key value
2. Additional information allowing to identify the owner of the public key (e-mail address, name ...)
3. A public key signature from a certification authority on all this information.

15 <http://www.references.modernisation.gouv.fr/rgs-securite>

Personal data protection must be integral part of data processing development in order to prevent any error, loss, unauthorised modification or any wrongful use of personal data in the applications.

### Basic measures

- Carry out data processing development in a data processing environment separate from that of production (for example, on different computers, in different datacenters).
- **Take into account security requirements regarding personal data as soon as the service is elaborated or as soon as the application is being designed.**

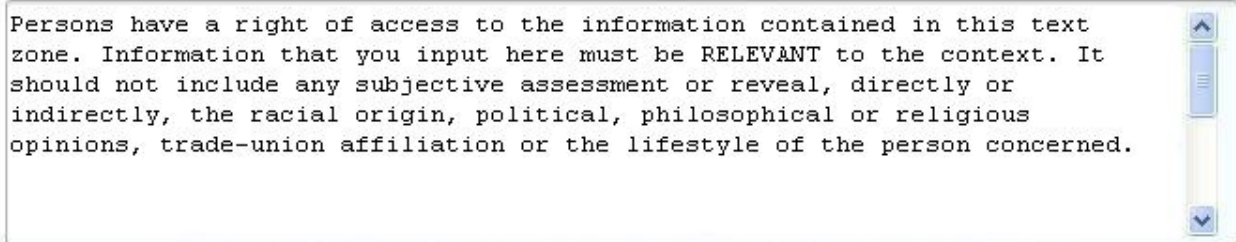
### What should be avoided

- **Use real personal data during the development and test phases.** Nevertheless if real data is required, it must be anonymised (Cf. Factsheet n°16 - Anonymisation)

### Further measures

- Development must entail **data acquisition and recording formats that minimize the collected** data. For example, when it comes to collecting the year of birth of a person, the corresponding form field should not allow the input of the month and day of birth. That could in particular be achieved by the implementation of a drop-down menu limiting the choices for a form field.
- Data formats must be compatible with the implementation of a retention period.
- Data **access control mechanisms** by categories of users must be integrated at development stage.
- Avoid resorting to free text input zones. When such zones are required, a digital watermark or as a pre-filled text (that erases itself as soon as the user decides to write in the zone) should show the following mentions:  
*Persons have a right of access to the information contained in this text zone. Information that you input here must be RELEVANT to the context. It should not include any subjective assessment or reveal, directly or indirectly, the racial origin, political, philosophical or religious opinions, trade-union affiliation or the lifestyle of the person concerned.*

Example:



Persons have a right of access to the information contained in this text zone. Information that you input here must be RELEVANT to the context. It should not include any subjective assessment or reveal, directly or indirectly, the racial origin, political, philosophical or religious opinions, trade-union affiliation or the lifestyle of the person concerned.

One sets apart **irreversible anonymisation** and **reversible anonymisation concepts**, the latter being sometimes referred as **pseudonymisation**.

Irreversible anonymisation consists in removing any identifying character from a set of data. Concretely, this means that all **directly and indirectly identifying** information is removed and makes it impossible any re-identification of the persons.

Reversible anonymisation is a technique which consists in replacing an identifier (or, more generally, personal data) with a *pseudonym*. This technique allows lifting the anonymity or the study of correlations where necessary.

### Basic measures

- Be very vigilant insofar as a re-identification can take place from partial information<sup>16</sup>.
- In order to anonymise personal data proceed as follows:
  - **generate a secret that is long enough and difficult to memorize**<sup>17</sup>;
  - apply a "one-way" function to the data: an algorithm suitable for such an operation is a keyed hash function such as the HMAC<sup>18</sup> algorithm based on SHA-1.
- If personal data is anonymised instead of simply being removed, there is a risk of re-identification<sup>19</sup>.
  - If there is no need to lift anonymity, it should be envisaged to destroy the secret in order to reduce this risk.
  - In the event that the secret must be preserved in order to possibly lift anonymisation or for the purpose of establishing correlations between various data, envisage **setting up of organisational measures**<sup>20</sup> in order to guarantee the **confidentiality of this secret**. Accesses to the secret must be traced.

### What should be avoided

- One must not use **anonymisation mechanisms that have not been validated by experts**. In particular a **good anonymisation algorithm** must:
  - **be irreversible**;
  - **present a very weak collision rate**: two different data should not lead to the same result;
  - present a **great dispersion**: two quasi-similar data must have very different results;
  - use a **secret key**.

### Further measures

- In some cases, it is advised to apply a **double reversible anonymisation**: that is to say the application of a second anonymisation on the result of a first anonymisation. **Both anonymisations must use different secrets, held by separate organisations**. The FOIN algorithm (Fonction d'Occultation des Informations Nominatives, Personal Information Hiding Function) is an example of algorithm using double anonymisation.

16 As an example, the place and date of birth can sometimes be sufficient to formally identify a person.

17 An example of character strings having the value of a secret is: f{rXan?cI\$IPcK|Bb-aQWH6ud0;#oQt\$.

18 HMAC is specified in document RFC 2104, <http://www.ietf.org/rfc/rfc2104.txt>

19 It is possible to associate the original data with the anonymised data as soon as the secret is compromised and that the complexity of the original data is not sufficient. Personal data often present a complexity, in other words insufficient entropy. For example, the French patronyms are in limited number (less than 1.5 million), and are all indexed.

20 An example of such measure consists in dividing the key in three components entrusted to three different persons, requiring that at least two persons meet to reconstitute the key.



**Encryption**, sometimes improperly referred to as encoding, is a cryptographic process making it possible to guarantee the confidentiality of information. Other cryptographic mechanisms allow ensuring the **integrity** of information, as well as the **authenticity** of a message by signing it.

Two cryptographic families used for encryption purposes can be differentiated: symmetric cryptography and asymmetric cryptography:

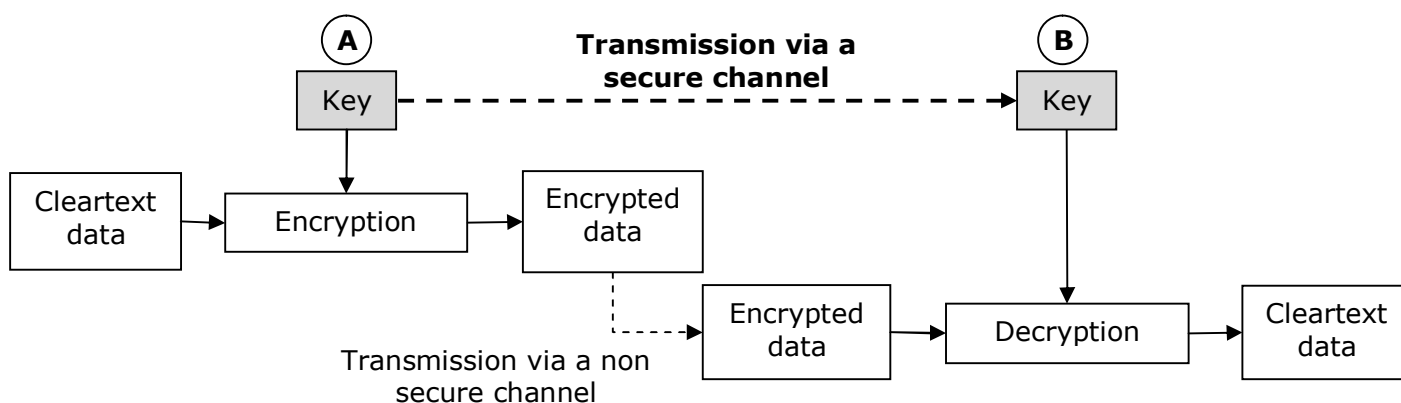
- Symmetric cryptography includes mechanisms for which the same key is used to encrypt and to decrypt data.
- Asymmetric cryptography includes mechanisms for which the key used for encryption, which is called the public key, is different from the key used to decrypt data, which is called the private key. A pair of keys must be used.

Asymmetric cryptography has multiple advantages:

- Each person only needs one pair of private/public keys. Conversely, symmetric cryptography calls for as many different keys as there are couples of people who want to communicate confidentially.
- Public keys can be made public for whoever wishes to send you a confidential message. However the authenticity of public keys is therefore not guaranteed. Hence, the implementation of asymmetric cryptography for the purpose of message exchange generally requires the implementation of a Public Key Infrastructure Management<sup>21</sup> System.

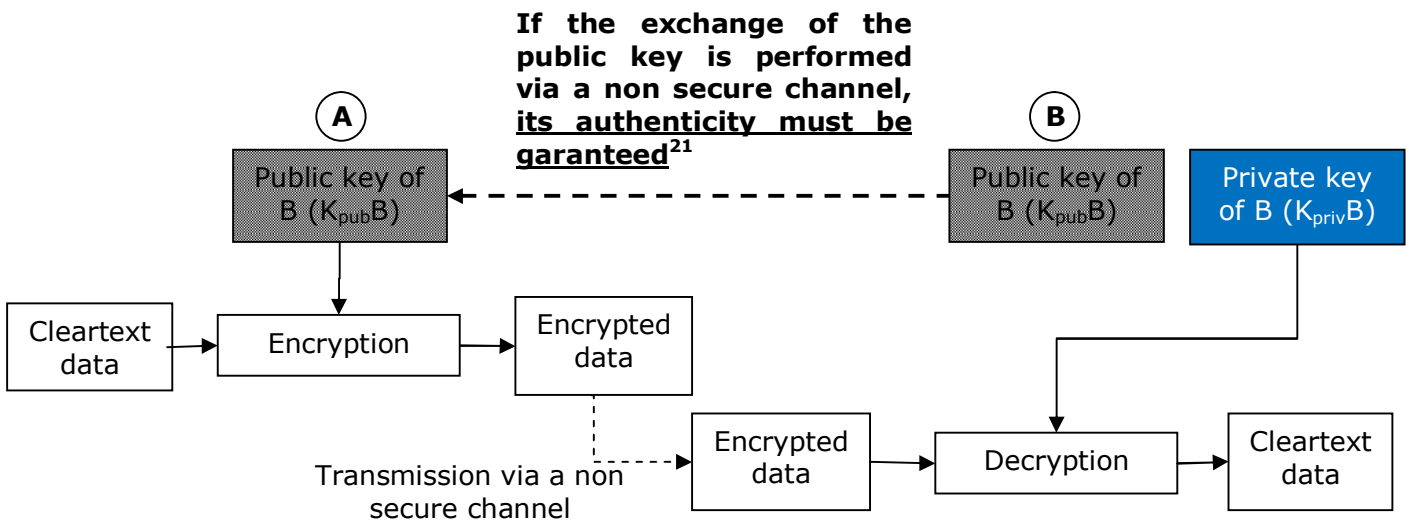
Confidential exchange of information between two parties A and B is carried out as follows:

Encrypting by means of symmetric cryptography:



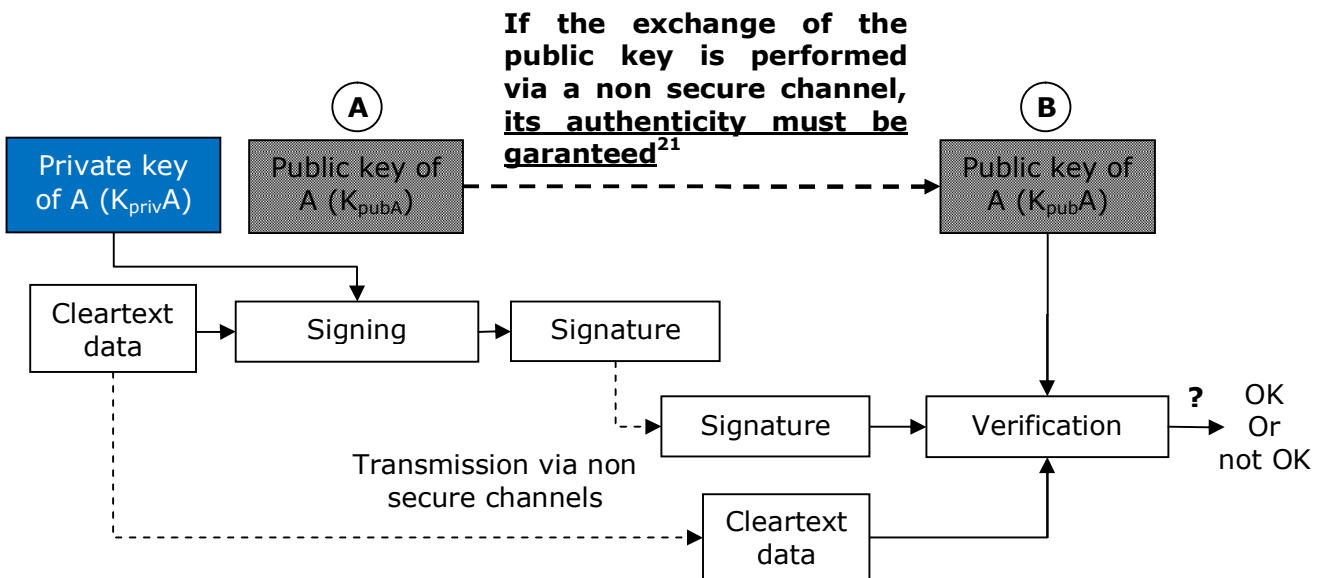
<sup>21</sup> Refer to Factsheet n° 14 – Information exchange with other organizations

Encrypting by means of asymmetric cryptography:



Signing by means of asymmetric cryptography:

Due to the fact that the private key is only held by a single person, asymmetrical cryptography allows guaranteeing the imputability of a message by signing it with the private key. This is not possible with symmetric cryptography since the key is shared between two parties.



21 Refer to Factsheet n° 14 – Information exchange with other organisations

## Basic measures

- Regarding symmetric encryption:
  - Use state of the art algorithms, such as AES or triple DES.
  - Use cryptographic keys lengths of at least 128 or 256 bits and which are not weak keys<sup>22</sup>. Moreover, generation of the keys must be done using tried and tested software programs, such as OpenSSL<sup>23</sup>.
- Regarding asymmetric encryption:
  - Use state of the art algorithms, such as RSA or ECC.
  - Regarding the keys length, it is advisable to follow the recommendations given in appendix B1 of the French General Security Reference Framework, Référentiel Général de Sécurité<sup>24</sup>. Moreover, generation of keys must be done by using tried and tested software programs, such as OpenSSL<sup>23</sup>.

## What should be avoided

- Use the simple DES algorithm which is considered as obsolete.
- Use cryptographic software or libraries that have not been verified by third parties with proven expertise.

## Further measures

- **Encryption of documents** can be achieved by means of various software programs, such as:
  - **TrueCrypt<sup>25</sup> software**, which allows the implementation of encrypted containers<sup>26</sup>.
  - **Gnu Privacy Guard software**, which allows the implementation of asymmetrical cryptography and one version of which is available at the address: <http://www.gnupg.org/index.fr.html>. It is suggested to select PGP DSA/EIGamal keys with a minimum size of 1536 bits, or RSA keys with a minimum size of 2048 bits.
  - Failing this, one can consider using a compression utility such as those based on the ZIP algorithm, since they allow encrypting by means of a password. This is the case in particular with the **7-Zip software**.

22 Example of a weak key is the null key:00000000000000000000000000000000

23 <http://www.openssl.org/>

24 Cf <http://www.references.modernisation.gouv.fr/rgs-secureite>

25 It is advisable to use version 6.0a which benefits from a first level certification by ANSSI.

26 By container, one means a file likely to contain several files.

# Acronyms

- AES:** Advanced Encryption Standard, a symmetrical cryptographic algorithm considered as a reference.
- DES:** Data Encryption Standard, a symmetrical cryptographic algorithm considered as outdated.
- DHCP:** Dynamic Host Configuration Protocol, a protocol allowing the dynamic configuration of the network parameters of equipment (including the attribution of its IP address).
- DNS:** Domain Name Server, These servers match in particular the name of machine, for example www.cnil.fr, with an IP address, as it happens 94.247.233.54.
- DSA:** Digital Signature Algorithm, a signature cryptographic algorithm.
- EBIOS:** An information security risk management methodology.
- ECC:** Elliptic Curve Cryptography, cryptography based on elliptic curves
- HMAC:** a chopping function allowing guaranteeing the authenticity of a message.
- HTTP:** HyperText Transfer Protocol, Web protocol.
- HTTPS:** HTTP secured by means of SSL.
- MAC:** Medium Access Control, the MAC address is a single identifier of each network interface.
- RAID:** Redundant Array of Independent Disks, indicates a technology making it possible to store data on several hard drives in order to improve fault-tolerance.
- RSA:** An asymmetrical cryptography algorithm, named after its three inventors, Rivest, Shamir and Adelman.
- SFTP:** a communications protocol functioning above SSH to transfer and manage remote files.
- SHA:** Secure Hash Algorithm, a family of standardized chopping functions (SHA-1, SHA256, etc. ...).
- SI:** Information system.
- SQL:** Structure Query Language, protocol being used for interrogating or handling data bases
- SSH:** Secure Shell, a secure protocol for remote connection in terminal mode.
- SSL:** Secure Socket To bush-hammer, a protocol which in particular allows securing HTTPS traffic.
- VNC:** Virtual Network Computer, a protocol allowing the remote control takeover of a workstation.
- VPN:** Virtual Private Network, a communication channel which guarantees the confidentiality of exchanges.

List of threats targeting information processing systems and files to be considered as a priority:

- **Regarding equipment:**
  - diversion from intended use (storage of personal files on an office computer, storage of sensitive documents on a USB key not suitable for that purpose ...);
  - spying (observation of a screen without the knowledge of its user, geolocalisation of a telephone ...);
  - going beyond operational limits (power failure, excessive temperature in a server room, full storage unit);
  - deterioration (flood or fire in a server room, degradation due to natural wear, vandalism ...);
  - modification (addition of peripherals, webcam, keylogger<sup>27</sup>...);
  - disappearance (theft, loss, transferring or discarding a computer ...).
- **Regarding software:**
  - diversion from the intended use (privilege escalation, search of contents, trace deletion...);
  - analysis (scanning of network addresses, acquisition of configuration data ...);
  - going beyond operational limits (injection of data outside intended values, buffer overflow ...);
  - total or partial suppression (logical bomb, code deletion ...);
  - modification (contagion by malicious code, inappropriate handling during a software update ...);
  - disappearance (transfer of an in-house developed software program, non-renewal of a license ...).
- **Regarding communication channels:**
  - passive eavesdropping (listening on a network cable, interception ...);
  - saturation (distant exploitation of a Wi-Fi network, unauthorised remote downloading, signal muffling ...);
  - degradation (severing wiring, fibber optic cable torsion ...);
  - modification (replacing a cable with another one that is not suitable, modification of cable tray ...),
  - disappearance (Theft of copper cables ...);
  - medium attack (man in the middle, replay / re-emission of traffic...).
- **Regarding paper documents:**
  - diversion from intended use (falsification, obliteration, use of reverse side of a paper document as a draft);
  - spying (reading, photocopying or photographing documents ...);
  - deterioration (natural ageing, chemical corrosion, wilful degradation, blaze during a fire);
  - disappearance (Theft of documents, resale, loss, loan, discarding ...).

---

<sup>27</sup> Device recording keyboard strokes



## Are you experiencing difficulties?

For further information visit the **CNIL** site at [www.cnil.fr](http://www.cnil.fr),

A legal information service is available  
everyday from **10:00 AM to 12:00 PM and 2:00 PM until 4:00  
PM** by calling **+33 1 53 73 22 22**

You can also send any request  
by fax to **+33 1 53 73 22 00**

# Assess the level of security for personal data within your organisation

Have you thought about the following?

↶ Factsheet		Measure	
1	Managing risks	Make an <b>inventory of</b> files, personal data and the their processing	<input type="checkbox"/>
		Identify the <b>threats</b> and their impacts on privacy	<input type="checkbox"/>
		Implement <b>security measures that are scaled</b> to the threats	<input type="checkbox"/>
2	Authenticating users	Define a <b>unique identifier (login)</b> for each user	<input type="checkbox"/>
		Adopt a <b>strict policy for user passwords</b>	<input type="checkbox"/>
		Make the user <b>change his/her password after it has been reset</b>	<input type="checkbox"/>
3	Authorisation management and awareness-raising	Define <b>authorisation profiles</b>	<input type="checkbox"/>
		Remove <b>obsolete access authorisations</b>	<input type="checkbox"/>
		<b>Document</b> operational procedures	<input type="checkbox"/>
		Write an <b>IT charter</b> and link it to <b>staff regulations</b>	<input type="checkbox"/>
4	Securing workstations	<b>Limit the number of attempts for accessing</b> an account	<input type="checkbox"/>
		Install a " <b>firewall</b> " software	<input type="checkbox"/>
		Use <b>regularly updated antivirus programs</b>	<input type="checkbox"/>
		Use an <b>automatic session locking mechanism</b>	<input type="checkbox"/>
5	Securing mobile data processing	Use encryption <b>measures for mobile computers</b> and removable storage units ( <b>USB keys, CD, DVD...</b> )	<input type="checkbox"/>
6	Backup and business continuity management	Perform <b>regular backups</b>	<input type="checkbox"/>
		Store the backup media in a secure location	<input type="checkbox"/>
		Implement security measures to protect the transportation of backups	<input type="checkbox"/>
		Define a <b>business continuity plan and test it regularly</b>	<input type="checkbox"/>
7	Supervising maintenance	<b>Record</b> maintenance <b>interventions in a register</b>	<input type="checkbox"/>
		<b>Erase</b> data from any equipment before it is <b>discarded</b>	<input type="checkbox"/>
		<b>Obtain the user's agreement prior to</b> any intervention on his/her workstation	<input type="checkbox"/>
8	Tracing accesses and managing incidents	Implement a system to <b>collect log files</b>	<input type="checkbox"/>
		<b>Inform the users</b> about the installation of the log files collecting system	<input type="checkbox"/>
		<b>Protect the log files collecting system</b> and the logs	<input type="checkbox"/>
		<b>Notify concerned people of any</b> fraudulent accesses to their data	<input type="checkbox"/>
9	Securing the premises	<b>Restrict the physical accesses</b> to the premises with <b>locked doors</b>	<input type="checkbox"/>
		Install <b>anti-intrusion alarms</b> and check them periodically	<input type="checkbox"/>
10	Securing the internal IT network	<b>Limit network traffic to what is strictly necessary</b>	<input type="checkbox"/>
		Secure distant accesses from mobile devices by <b>VPN</b>	<input type="checkbox"/>
		Use SSL protocol with a128 bits key for <b>Web services</b>	<input type="checkbox"/>
		Use the WPA- AES/CCMP protocol for WiFi networks	<input type="checkbox"/>
11	Securing servers and applications	Adopt a <b>strict policy for administrator passwords</b>	<input type="checkbox"/>
		Install <b>critical updates</b> without delay	<input type="checkbox"/>
		Ensure data <b>availability</b>	<input type="checkbox"/>
12	Managing subcontractors	Envisage a <b>specific clause</b> in the subcontractors contracts	<input type="checkbox"/>
		Ensure the effectiveness <b>of the planned guarantees</b> (safety audits, visits...)	<input type="checkbox"/>
		Define the <b>conditions for data restitution and destruction</b>	<input type="checkbox"/>
13	Archiving	Implement specific access methods to the archived data	<input type="checkbox"/>
		Destroy obsolete files in a secure way	<input type="checkbox"/>
14	Securing exchanges with other organisations	<b>Encrypt</b> data prior to sending it	<input type="checkbox"/>
		Ensure it is to the <b>proper recipient</b>	<input type="checkbox"/>
		Transmit <b>secret</b> through a distinct message and through a different channel	<input type="checkbox"/>