THE CNIL'S GUIDES - 2018 EDITION

SECURITY OF PERSONAL DATA

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

TABLE OF CONTENTS

SECURITY OF PERSONAL DATA

INTRODUCTION

Risk management allows to determine the precautions to take ***"with regard to the nature of the data and the risks of the processing,*** *to preserve the security of the data..."* (article 34 Act of 6th January 1978, known as the act on "Information technology, Data files and Civil Liberties" – hereafter referred to as the French Data Protection and Freedoms Act or FDPFA). The 2016/679 European regulation of 27th April 2016 (known as "General Data Protection Regulation" or GDPR) specifies that protecting personal data requires taking *"appropriate technical and organisational measures to ensure* ***a level of security appropriate to the risk"*** (article 32).

Such an approach allows for objective decision making and the determination of the measures strictly necessary and suitable to the context. It is, however, often difficult, when you are not familiar with these methods, to apply such an approach and to ensure that the required measures have indeed been implemented.

To help you with complying with your legal obligations, **this guide lists the basic precautions which should be implemented systematically.**

Ideally, this guide will be used in a risk management context, however minimal, which includes the following four stages:

Listing the processing of personal data, whether automated or not, the data processed (e.g.: *customer files, contracts) and the media on which they rely:*

- the hardware (e.g.: servers, laptops, hard drives);
- the software (e.g.: operating system, business software);
- the communication channels (e.g.: fibre optic, Wi-Fi, Internet);
- the paper documents (e.g.: printed documents, photocopies).

Assessing the risks generated by each processing operation:

1. **Identifying the potential effects** on the rights and freedoms of individuals concerned, for the three following feared events:
   - **illegitimate access to data** (e.g.: identity theft following the divulging of pay slips of all of the employees of a company);
   - **unwanted modification of data** (e.g.: wrongly accusing an individual of a mistake or a crime following the modification of access logs);
   - **temporary or definitive unavailability of data** (e.g.: not detecting a drug interaction due to it being impossible to access the patient's electronic medical record).

2. **Identifying the sources of risks** (who or what could be the cause of each feared event?), taking into consideration internal and external human sources (e.g.: the IT administrator, the user, external attacker, competitor) and internal and external non-human sources (e.g.: water, hazardous materials, non-targeted computer virus).

3. **Identifying the possible threats** (what could allow each feared event to occur?). These threats occur via the media on which data rely (hardware, software, communication channels, paper media, etc.) which can be:
   - used in an inappropriate way (e.g.: rights abuse, handling error);
   - modified (e.g.: trapped software or hardware - keylogger, installing malicious software);
   - lost (e.g.: theft of a laptop, loss of a USB stick);
   - observed (e.g.: viewing of a screen on a train, geo-location of an equipment);
   - damaged (e.g.: vandalism, degradation due to natural wear);
   - overloaded (e.g.: full storage medium, denial of service attack).

4. **Determining the existing or planned measures** which allow for each risk to be dealt with (e.g.: controlling access, backups, traceability, security of the premises, encryption, or anonymisation).

5. **Evaluating the severity and likelihood** of the risks, with regard to the previous elements (an example of a scale that can be used for the evaluation: negligible, moderate, significant and maximal).

The following table can be used to formalise this consideration:

Risks	Effects on individuals	Main sources of risks	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access to data						
Unwanted modification of data						
Loss of data						

Implementing and checking the planned measures. If the existing and planned measures are judged appropriate, it is advisable to ensure that they are applied and tested.

Carrying out periodical security audits. Each audit must produce an action plan, the implementation of which should be monitored at the highest level of the organisation.

FURTHER MEASURES

- The GDPR introduces the notion of a "*data protection impact assessment*", also known as "Privacy Impact Assessment" and specifies that it must, at the least, contain "*a description of the processing and its purposes, an assessment of the necessity and proportionality, an assessment of the risks [...] and the measures envisaged to address the risks, and comply with the regulations*" (see article 35.7). **This reflexion process regarding the risks could help to fill in the section on the risk assessment of the privacy impact assessment.**
- The PIA guides from the CNIL (https://www.cnil.fr/fr/PIA-privacy-impact-assessment) offer a complete guide for the realisation of data protection impact assessment.
- **Information security risk management**[1] **can be carried out at the same time as privacy risk management** since these approaches are compatible.
- The risk analysis allows to determine the security measures that have to be implemented. **Allocating a budget** for their implementation is required.

1 For example, with the help of the EBIOS method, a risk management method published by the "Agence nationale de la sécurité des systèmes d'information – ANSSI" (the French National Cybersecurity Agency) of the "Secrétariat général de la défense et de la sécurité nationale - SGDSN" (General Secretariat for Defence and National Security). EBIOS is a registered trademark of SGDSN (https://www.ssi.gouv.fr/entreprise/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/).

1 RAISING USER AWARENESS

Make each user aware of the privacy and security challenges of the organisation.

BASIC PRECAUTIONS

- **Raise the awareness of users working with personal data by educating them on the privacy risks,** inform them of the measures implemented by their organisation in order to deal with the risks and their potential consequences. Organise awareness raising sessions, regularly send updates on the relevant procedures for the individuals' roles, send them reminders via e-mail, etc.
- **Document the operating procedures,** keep them up to date and make them available to all the users concerned. In concrete terms, any action on personal data, whether it is administration-related operations or plain use of an application, must be explained in clear language adapted to each user category, in documents to which the users can refer.
- **Write an IT charter and enforce its application**. This charter should, at the least, include the following elements:

1. A reminder of the rules of data protection and of sanctions incurred in the event of non-compliance with these rules.
2. The scope of the application of the charter, which should include in particular:
   - methods of intervention of the teams in charge of managing IT resources for the organisation;
   - authentication means used by the organisation;
   - security rules which users must conform to, including:
     - informing the internal IT department about any suspected data breach or attempt to violate your IT user account and generally any dysfunction;
     - never entrusting your identifier/password to a third party;
     - never installing, copying, editing or destroying software without authorisation;
     - locking computers as soon as users leave their workstation;
     - never accessing, trying to access, or remove information if it does not relate to the tasks performed by the user;
     - respecting the procedures defined beforehand by the company in order to supervise data transfer on mobile media, notably by obtaining prior authorisation from the supervisor and by complying with the security rules.
3. The procedures for the use of IT equipment and telecommunication resources available to the user such as:
   - workstations;
   - mobile equipments (especially in the context of telecommuting);
   - individual storage spaces;
   - local networks;
   - personal devices (expecially the conditions to use such devices);
   - the Internet;
   - electronic messaging;
   - telephony.

1 RAISING USER AWARENESS

4. The information system administration conditions, and, if required, the existence of:
- automatic filtering systems;
- automatic logging systems;
- workstation management.

5. Responsibilities and sanctions incurred in the event of non-compliance with the charter.

FURTHER MEASURES

- Implement an **information classification** policy defining several levels of classification and requiring to mark the documents and e-mails containing confidential data.
- Place a visible and explicit notice on each page of paper or electronic documents which contain sensitive data[2].
- Organise training and awareness raising sessions on information security. Send periodic reminders via electronic messaging.
- Arrange for the signature of a **confidentiality agreement** (see typical clause herein below), or include in the employment contracts a **specific confidentiality clause** concerning personal data.

Sample confidentiality agreement for those responsible for handling personal data:

I, undersigned, Mr. / Mrs. _____, employed as _____ employed as _____ Company (hereinafter named as "the Company"), being in that capacity involved in access to personal data, state that I acknowledge the confidentiality of the aforementioned data.

Therefore, I am committing, in accordance with articles 34 and 35 of the modified Act of 6th January 1978 regarding information technology, data files and civil liberties, as well as articles 32 to 35 of the General Data Protection Regulation of 27th April 2016, to taking all precautions in accordance 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 stop it being communicated to persons not expressly authorised 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 that are a part of my duties;
- only revealing this data to the duly authorised persons, due to their capacity to receive it, whether they are private, public, physical or moral persons;
- not making any copy of this data except when it is necessary to carry out my duties and responsibilities;
- taking all measures in accordance with the uses and the state of the art within the context of my duties in order to prevent the devious or fraudulent use of this data;
- taking all precautions in accordance with the uses and the state of the art to preserve the physical and logical 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;
- in the event of termination 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 termination 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 existing regulations, notably in terms of articles 226-16 to 226-24 of the criminal code.

Issued in xxx, on xxx, with xxx copies

Name:
Signature:

2 Sensitive data are defined by article 8 of the French Data Protection and Freedoms Act, and article 9 of the General data protection regulation.

2 AUTHENTICATING USERS

Recognising your users to manage their access rights.

To ensure that a user only accesses the data that he/she needs, he/she must be associated with a unique identifier and must authenticate himself/herself before any access to personal data.

Authentication factors are grouped into three families according to:
- **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 digital fingerprint or a handwritten signature. As a reminder, the Act on Information Technology and Civil Liberties subordinates the use of biometrics to a CNIL preliminary authorisation[3].

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

BASIC PRECAUTIONS

- **Define a unique identifier per user and prohibit shared accounts** between several users. In the event that using generic or shared identifiers is unavoidable, require explicit confirmation from the management and implement measures to log their activities.
- **Respect the CNIL recommendation[4] when passwords are used for authentication,** notably by storing the passwords in a secure way and applying the following complexity requirements to them:
  - be at least **8 characters long including 3 out of 4 types of characters** (uppercase, lowercase, numbers, special characters) if the authentication includes a measure restricting access to the account like:
    - temporary lockdown of the account after several failed attempts,
    - a "Captcha",
    - the locking of the account after 10 failed attempts;
  - **have 12 characters minimum** and **4 types of character if the authentication only relies on a password;**
  - have over **5 characters** if the authentication requires some additional confidential information. **For the additional information,** use a **confidential identifier that is at least 7 characters long** and **block the account on the 5th** unsuccessful attempt;
  - the password can be just **4 characters** if the authentication relies on equipment held by the individual and if the password **is only** used to unlock the physical device held by the individual himself/herself (for example a smart card or mobile phone) and that the device is **blocked on the 3rd** unsuccessful attempt.

Mnemonic methods enable complex passwords to be created, for example by:
- using only the first letter of the words in a sentence;
- uppercasing if the word is a noun (e.g.: **C**hief);
- keeping punctuation marks (e.g.: ');
- expressing numbers as figures from 0 to 9 (e.g.: One → 1);
- using phonetics (e.g.: ate → 8).

For example, the sentence: "**one f**orewarned **C**hief **T**echnical **O**fficer **i**s **w**orth **t**wo" corresponds to the password **1fCTOiw2.**

3 To this end, see the dedicated article "Biométrie : un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail" (Biometrics a new framework for controlling biometric access to workplaces) on our website https://www.cnil.fr/fr/biometrie-un-nouveau-cadre-pour-le-controle-dacces-biometrique-sur-les-lieux-de-travail

4 https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

2 AUTHENTICATING USERS

When he or she first logs in, require the user to change any password **attributed by an administrator or automatically** by the system when creating an account or resetting a password.

WHAT SHOULD BE AVOIDED

- Communicating your own password to anyone.
- Storing passwords in an unencrypted file, on a paper or in a location easily accessible by other people.
- Saving passwords in the browser without using a master password.
- Using passwords with a link to personal information (name, date of birth, etc.).
- Using the same password for accessing different accounts.
- Keeping the default password.
- Sending your own passwords via email.

FURTHER MEASURES

- **Favour strong authentication** when possible.
- **Reduce the allowed number of access attempts** to user accounts on workstations and temporarily block the account when the limit is reached.
- **Require passwords to be updated** at a relevant and reasonable frequency.
- Implement technical measures **to ensure the respect of the rules relating to authentication** (for example: blocking an account if a password is not updated).
- If possible, avoid making the identifiers (or logins) of users the same as accounts defined by default by the software companies and deactivate default accounts.
- **Use password managers to have different passwords for each service,** while only keeping one master password (https://www.cnil.fr/fr/construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces).
- **Store passwords securely,** at the least hashed with a cryptographic hash function using a salt or a key, and, optimally, transformed with a specific function designed for this purpose using a salt or a key[5] (see *Factsheet n°. 17*). A key must not be stored in the same database as the fingerprints of the passwords.
- Refer to the *rules and recommendations concerning authentication mechanisms* published by the ANSSI when strong authentication mechanisms are implemented, notably its appendices B3[6] and B1[7] dealing respectively with *authentication mechanisms and cryptographic mechanisms*.

5 The random used is called a "salt" when it is different for each password stored and a "key" when it is common to the hash of all of the passwords (for example a whole database).
6 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf.
7 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf.

3 ACCESS MANAGEMENT

Only allow access to data that the user really needs.

BASIC PRECAUTIONS

- **Define the authorisation profiles** in the systems by separating the tasks and area of responsibility, in order to restrict users' access to the only data strictly necessary for fulfilling their responsibilities.
- **Withdraw the users' access rights as soon as they are no longer authorised to access a room or an IT resource, as well as at the end of their contract.**
- **Carry out an annual review of the access rights** in order to identify and remove unused accounts and realign the rights and the role of each user.

WHAT SHOULD BE AVOIDED

- Creating or using shared accounts for several users.
- Granting administrator rights to users who do not need them.
- Granting a user more privileges than necessary.
- Forgetting to remove temporary authorisations granted to a user (for a replacement, for example).
- Forgetting to delete user accounts of individuals who have left the organisation or changed role.

FURTHER MEASURES

Establish, document and regularly review an **access control policy** that is proportionate to the processing implemented by the organisation. The access control policy must include:

- the procedures to be applied automatically upon arrival and departure or a change of role for an individual with access to personal data;
- the planned consequences for individuals with legitimate access to data in the event of non-compliance with security measures;
- the measures allowing to restrict and control the granting and use of access to processing (see *Fact-sheet n°. 4: Logging access and managing incidents*).

4 LOGGING ACCESS AND MANAGING INCIDENTS

Log access and organise incident management procedures to manage incidents allowing to react in the event of data breach (breach of confidentiality, integrity or availability).

In order to be able **to identify fraudulent access** or **abusive use** of personal data, or to determine the origin of an incident, it is necessary to log certain actions carried out on the IT systems. To do this, logging and incident management measures must be implemented. It must **record relevant events** and guarantee **that these logs cannot be altered.** In any cases, **these elements must not be kept for an excessive time period.**

BASIC PRECAUTIONS

- **Set up logs** (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 a particularly significant risk for the data subjects);
  - **as a minimum, the users' accesses should be logged** with their identifier, the date and time of their connection as well as the date and time of their disconnection;
  - in certain cases, it may be necessary to also keep information on the actions undertaken by the user, the types of data consulted and/or modified, and the reference of the concerned data.
- **Inform the users** of the installation of such a system, after informing and consulting with personnel representatives.
- **Protect the logging equipments and the logged information** against unauthorised access, notably by making it inaccessible to the individuals whose activity is logged.
- Set up procedures detailing the monitoring of processing use and **periodically carry out a review of the logged information** to detect possible anomalies.
- Ensure that **those in charge of the logging management notify the data controller, as soon as possible, of any anomaly or security incident.**
- **Notify the CNIL or the competent Data Protection Authority of any personal data breach and,** except as otherwise provided by the GDPR[8], **also notify the individuals concerned** so that they can limit the consequences of this.

WHAT SHOULD BE AVOIDED

- Using information coming from the logs for another purpose than guaranteeing the proper use of the information processed (for example: using the logs to count the hours worked is a misuse, punishable under the law).

FURTHER MEASURES

- See the security recommendations for the implementation of a logging system published by the ANSSI at the following address: : https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/

8 articles 33 and 34 of the GDPR

5 SECURING WORKSTATIONS

Prevent fraudulent access, the execution of viruses or remote-control takeover, in particular via the Internet.

The risks of an intrusion into information systems are significant and workstations are one of the main points of entry.

BASIC PRECAUTIONS

- Implement an **automatic logout** procedure to lock any workstation not-used for a given period of time.
- **Install a firewall** and limit authorised communication ports to those that are strictly necessary for the proper operation of the applications installed on the workstation.
- Use **regularly updated antivirus software** and define a **policy imposing regular updates of the softwares.**
- Configure softwares so that the **security updates are carried out automatically** when possible.
- **Favour storing users' data on a storage medium that is regularly backed-up and accessible via the network of the organisation** rather than on the workstations themselves. In the event that data is stored locally, provide synchronisation or backup measures to users and train them in their use.
- **Limit the connection of mobile media** (USB sticks, external hard drives, etc.) to what is essential.
- Disable autorun for removable media.
- For **assistance on workstations:**
  - remote administration tools must **collect** the user's **consent** before any intervention on his/her workstation, for example, by answering a message which is displayed on the screen;
  - the user must also be able to **notice if remote control is going on** and when it has finished, e.g. thanks to the displaying of a message on the screen.

WHAT SHOULD BE AVOIDED

- Using obsolete operating systems (see the list at https://www.cert.ssi.gouv.fr/information/CERTFR-2005-INF-003/).
- Granting administrator rights to users who do not have competencies in IT security.

FURTHER MEASURES

- **Prohibit the running of downloaded applications** not coming from safe sources.
- **Limit the use** of applications requiring administrator rights.
- **Securely delete data present on a workstation prior to reassign it** to another individual.
- **In the event that a workstation is compromised, look for the source as well as any trace of an intrusion** in the IT system of the organisation, in order to detect if other elements have been compromised.
- **Carry out security monitoring of software and hardware used in the IT system of the organisation.** The CERT-FR (Computer Emergency Response Team) publishes warnings and advice on vulnerabilities discovered in software and hardware on its website (http://cert.ssi.gouv.fr/) and provides, where possible, the means to protect against them.
- **Update applications** when critical flaws have been identified and corrected.
- Install, without delay, **operating systems' critical updates by** scheduling a weekly automatic verification.
- Make all users aware of **the behaviour to adopt and the list of individuals to contact in the event of a security incident or the occurrence of an unusual event** affecting the information and communication systems of the organisation.
- See the document from the CERT-FR on the right reactions in the event of an intrusion in the information system, accessible at the following address: http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html.

6 SECURING MOBILE DATA PROCESSING

Anticipate data breach following the theft or loss of a mobile equipment.

The increase use of laptops, USB sticks and smartphones makes it necessary to prepare for data breach following the theft or loss of such equipment.

BASIC PRECAUTIONS

- **Raise users' awareness on the specific risks associated with using mobile tools** (e.g.: theft of equipment) and the planned procedures to reduce these risks.
- **Implement controlled backup or synchronisation measures** for mobile workstations, in order to protect against the loss of stored data.
- **Provide encryption measures protecting mobile workstations and mobile storage media** (laptop, USB sticks, external hard drives, CD-ROMs, DVD-RWs, etc.), for example:
  - encryption of the hard drive in its entirety when the operating system offers such a functionality;
  - individual file by file encryption;
  - creation of encrypted containers (a file containing other files and folders).

  Many laptops include functionalities allowing to encrypt their hard drive: whenever possible, it is advisable to use this feature.
- **Regarding smartphones, in addition to the PIN code for the SIM card, activate automatic locking of the terminal and require a confidential piece of information to unlock it** (password, pattern, etc.).

WHAT SHOULD BE AVOIDED

- Using cloud services installed by default on a device as a backup or synchronisation tool without doing an in-depth analysis of their terms of use as well as of their security guarantees. These are generally not able to respect the advice given in *Factsheet n°. 13: Managing subcontracting.*

FURTHER MEASURES

- **Place a privacy filter** on the screens of workstations used in public places.
- **Limit the storage of data** on mobile workstations to what is strictly necessary, and possibly prohibit it during trips abroad (see the "Passeport de conseils aux voyageurs" (passport advice to travellers document) published by the ANSSI https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf).
- **Implement protection measures against theft (**e.g. security cable, visible marking of equipment) **and ones to reduces its effects** (e.g. automatic locking, encryption).
- When mobile devices are used to collect data on the go (e.g.: personal assistants, smartphones, laptops, etc.), encrypt the data on the terminal. Also put in place device locking after a few minutes of inactivity and the purging of data collected as soon as it is transferred to the IT system of the organisation.

7 PROTECTING THE INTERNAL NETWORK

Only authorise the network functions required for the processing implemented.

BASIC PRECAUTIONS

- **Limit Internet access** by blocking non-essential services (VoIP, peer to peer, etc.).
- **Manage the Wi-Fi networks.** They must use state of the art encryption (WPA2 or WPA2-PSK with a complex password) and networks open to guests must be separate from the internal network.
- **Require a VPN for remote access,** as well as, if possible, a strong authentication of the user (smart card, one-time password generating device (OTP), etc.).
- **Ensure that no administration interface is directly accessible from the Internet.** Remote maintenance must be carried out via a VPN.
- **Limit network traffic to the bare essentials** by filtering the incoming/outgoing traffic on equipment (firewall, proxy, servers, etc.). For example, if a web server uses HTTPS, you must only authorise the incoming traffic on this machine via port 443 and block all the other ports.

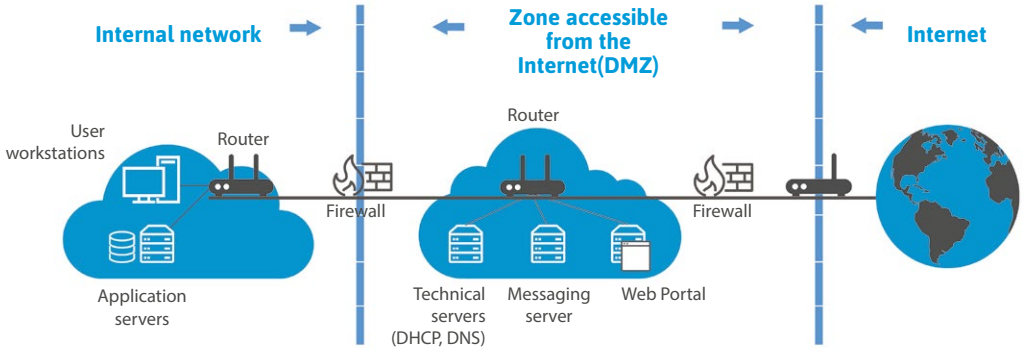
WHAT SHOULD BE AVOIDED

- Using the telnet protocol for the remote connection to active network equipment (firewall, routers, and switches). Instead, it is advisable to use SSH or a direct physical access to the equipment.
- Providing users with unfiltered Internet access.
- Setting up a Wi-Fi network using a WEP encryption.

FURTHER MEASURES

- **The ANSSI has published[9] recommendations** for the securing of websites[10], TLS[11] and Wi-Fi[12].
- **You can implement the automatic identification of equipment** by using network card identifiers (MAC addresses) in order to prohibit connections from an unlisted device.
- **Intrusion detection systems** (IDS) can analyse the network traffic to detect attacks. Users must be notified when their content is analysed.
- **Network partitioning** reduces the impacts in the event of a compromise. An internal network, on which no connection coming from the Internet is authorised, and a DMZ (DeMilitarized Zone) network, accessible from the Internet, can be distinguished by separating them with gateways (firewalls).

Example of the implementation of a DMZ



9 https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
10 https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/
11 https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/
12 https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/

8 SECURING SERVERS

Strengthen the security measures applied to servers.

The security of servers must be a priority as they centralise a large amount of data.

BASIC PRECAUTIONS

- **Only allow qualified individuals to access the tools and administration interfaces.**
- Use accounts with less privileges for common operations.
- **Adopt a specific password policy** for administrators. Change passwords, at the least, following each departure of an administrator and if a compromise is suspected.
- **Install critical updates** without delay for both operating systems and applications, by scheduling a weekly automated verification.
- In terms of database administration:
  - **use personalised account identifiers** to access databases and create specific accounts for each application;
  - implement measures against attacks via the injection of SQL code, scripts, etc.
- **Carry out backups and check them regularly.**
- **Implement the TLS protocol** (replacing SSL[13]), or another protocol ensuring encryption and authentication, as a minimum for any online data exchange and verify its proper implementation via the appropriate tools[14].

WHAT SHOULD BE AVOIDED

- Using unsecured services (cleartext authentication, cleartext flow, etc.).
- Using servers hosting databases for other functions, notably to browse websites, access electronic messaging, etc.
- Placing databases directly on a server accessible from the Internet.
- Using generic user accounts (in other words shared between several users).

FURTHER MEASURES

- The CNIL Recommendation[15] on passwords lists the best practices to adhere to.
- Any system processing sensitive data[16] must be set up in a **dedicated environment (**isolated).
- Server **administration operations** should be carried out via a **dedicated and isolated network,** accessible only after **strong authentication** and with **enhanced traceability.**
- When it comes to software being executed on servers, use **vulnerability detection tools** (vulnerability scanners such as nmap[17], nessus[18], nikto[19], etc.) for the most critical processing, in order to detect potential security flaws. Attack detection and prevention on critical systems or servers can also be used.
- Restrict or prohibit physical and logical access to diagnostic and remote configuration ports.
- **The ANSSI has published various recommendations[20] on its website** among which some aim at securing the administration of IT systems[21] and best practice in terms of securing Active Directory servers[22].

13 The TLS protocol is often called SSL or SSL/TLS, "SSL" being the name given to this protocol for its first versions considered today as vulnerable and to be avoided.
14 For TLS, there is, for example, https://www.ssllabs.com/ssltest/ or https://ssl-tools.net/
15 https://www.cnil.fr/fr/mots-de-passe-des-recommandations-de-securite-minimales-pour-les-entreprises-et-les-particuliers
16 Sensitive data is described in article 8 of the FDPFA and article 9 of the GDPR.
17 https://nmap.org/
18 http://www.nessus.org
19 http://www.cirt.net/nikto2
20 https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/.
21 https://www.ssi.gouv.fr/entreprise/guide/securiser-ladministration-des-systemes-dinformation/
22 https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

9

SECURING WEBSITES

Ensure that the basic best practices are applied to websites.

Every website must guarantee its identity and the confidentiality of the information it sends or it collects.

BASIC PRECAUTIONS

- **Implement the TLS protocol** (replacing SSL[23]) on all websites, by using only the most recent version and by checking its proper implementation.
- **Make the use of TLS compulsory** for all pages including forms collecting personal data or allowing authentication of the user and ones on which non-public personal data is displayed or transmitted.
- **Limit the communication ports** to those strictly required for the proper functioning of the applications installed. If a web server only accepts HTTPS connections, only IP network traffic entering this machine on port 443 must be authorised and all other ports must be blocked.
- **Only allow qualified individuals access to tools and administration interfaces.** In particular, limit the use of administrator accounts to teams in charge of IT and only for the administration actions which require it.
- **If cookies not required by the service are used, collect consent** from the Internet user after informing him or her and before the cookie is deposited.
- **Limit the number of components implemented,** carry out monitoring on them and keep them up-to-date.

WHAT SHOULD BE AVOIDED

- Transferring personal data via a URL such as identifiers or passwords.
- Using unsecured services (cleartext authentication, cleartext flow, etc.).
- Using severs hosting databases or severs as workstations, especially to browse websites, access electronic messaging, etc.
- Placing databases on a server directly accessible from the Internet.
- Using generic user accounts (in other words shared between several users).

FURTHER MEASURES

- Concerning the setting up of cookies, it is advisable to consult the "*Site web, cookies et autres traceurs*" (Websites, cookies and other trackers) file on the website of the CNIL: https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs.
- When it comes to software being executed on servers, it is advisable to use **vulnerability detection tools** (vulnerability scanners such as nmap, nessus, nikto, etc.) for the most critical processing, in order to detect potential security flaws. Attack detection and prevention on critical systems or servers can also be used. These tests must be carried out regularly and before any production launch of a new software version.
- **The ANSSI has published specific recommendations on its website**[24] in order to implement TLS[25] and to secure a website[26].

23 The TLS protocol is often called SSL or SSL/TLS, "SSL" being the name given to this protocol for its first versions considered today as vulnerable and to be avoided.
24 https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
25 https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/
26 https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/

10

ENSURING CONTINUITY

Carry out regular backups to reduce the effect of undesired loss of data.

Backup copies must be made and tested regularly. A business continuity plan anticipating possible incidents (e.g.: hardware failure) must be prepared.

BASIC PRECAUTIONS

- **Regarding data backup**
  - **Carry out frequent data backups,** whether they are in paper or electronic form. It might be appropriate to perform incremental backups on a daily basis and complete backups[27] at regular intervals.
  - **Store the backups on an external site,** if possible in waterproof and fireproof safes.
  - Protect backed up data **with the same security level as data stored on operational servers** (for example, by encrypting the backups, by organising storage in a safe place or by contractually regulating an outsourced backup service).
  - When the backups are sent via the network, it is advisable to encrypt their transmission channel if it is not within the organisation.
- **Regarding business continuity management**
  - **Create an IT business continuity management plan,** even if brief, including the list of those involved.
  - **Ensure that users, service providers and sub-contractors know who to warn in the event of an incident.**
  - **Regularly test the restoring of backups and the application of the business continuity management plan.**
  - Regarding equipment:
    - use an uninterruptible power supply to protect the equipment used for critical processing;
    - put in place storage unit redundancy, by using a RAID technology[28] for example.

WHAT SHOULD BE AVOIDED

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

FURTHER MEASURES

- Concerning the establishment of a business continuity management plan, the SGDSN has published a guide available at the following address: https://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf.
- If the demands on the availability of data and systems are high, it is advisable to establish data copying to a secondary site.

27 An incremental backup consists of only recording the modifications made after a previous backup.
28 RAID (Redundant Array of Independent Disk) 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.

11

ARCHIVING SECURELY

Archive data which is no longer used on a daily basis, but which has not yet reached the end of its data retention period, for example because it is kept to be used in the event of litigation.

Archives must be secured, especially if the archived data is sensitive data or data which could have serious impacts on the data subjects.

BASIC PRECAUTIONS

- **Define an archive management procedure:** what data must be archived, how and where is it stored, how is descriptive data managed?
- **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.
- With regard to the destruction of archives, **select a procedure guaranteeing that the archive has been destroyed in its entirety.**

WHAT SHOULD BE AVOIDED

- Using media that does not have a sufficient guarantee in terms of longevity. For example, the longevity of rewritable CDs and DVDs seldom exceeds four or five years.
- Keeping data in an active database while simply noting it as archived. Archived data must only be accessible to a specific department in charge of accessing it.

FURTHER MEASURES

- The CNIL has published a recommendation[29] concerning electronic archiving methods.
- Data presenting a historic, scientific or statistical interest justifying that it is not destroyed is governed by the rules contained in book II of the "Code du Patrimoine" (French Heritage Code). More detailed information on archiving issues is available on the website of Archives de France (National Archives). See the article on the longevity of digital information[30].
- In conjunction with the "Direction générale des patrimoines du ministère de la Culture" (General Heritage Department of the Ministry of Cultural Affairs), the CNIL has published the Single Authorisation n°. 29[31] which covers the processing of archive services relating to public information containing personal data.
- The delegate and the "comité interministériel aux archives de France" (inter-ministerial committee at France's National Archives) organise and coordinate the action of the public authorities in terms of archives. In this context they have published different documents and frameworks, including the general framework for archive management available at the following address: http://www.gouvernement.fr/delegue-et-comite-interministeriel-aux-archives-de-france.

29 https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017651957
30 https://francearchives.fr/fr/article/26287479
31 https://www.cnil.fr/fr/declaration/au-029-archives-publiques

12

SUPERVISING MAINTENANCE AND DATA DESTRUCTION

Guarantee data security at all times in the life cycle of hardware and software.

Maintenance operations must be supervised to control access to data by service providers. Data must be deleted before discarding hardware.

BASIC PRECAUTIONS

- **Record maintenance in a register.**
- Include a security clause into the maintenance contracts undertaken by service providers.
- **Have a responsible person from the organisation supervise work by third parties.**
- Write and implement a **secure data deletion procedure.**
- **Securely delete data from hardware before it is discarded, sent for repair by a third party** or at the end of a rental contract.

WHAT SHOULD BE AVOIDED

- Installing applications for remote maintenance with known vulnerabilities, for example, ones which do not encrypt communications.
- Reusing, reselling or disposing of media that has contained personal data that have not been securely deleted.

FURTHER MEASURES

- Use dedicated data deletion software which has been audited or certified. The ANSSI grants first level certifications[32] to software of this kind.

An example of a clause that can be used in the case of maintenance by a third party:

Each maintenance action will have to be described with the dates, nature of operations and names of the intervening parties, and 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 obtain prior consent from X before each remote maintenance operation for which he/she would take the initiative.

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

NB: This maintenance clause must be coupled with one dealing with confidentiality for subcontracting.

32 https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/

13

MANAGING DATA PROCESSORS

Supervise data security with subcontractors.

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

BASIC PRECAUTIONS

- **Only use subcontractors which are able to provide sufficient guarantees** (in particular in terms of specialised knowledge, reliability and resources). Require service providers to communicate their information system security policy before signing a contract with them.
- Take and document the means (security audits, installation visits, etc.) used to **ensure the effectiveness of the guarantees offered by the subcontractor** in terms of data protection. These guarantees include:
  - encryption of data according to its sensitivity or, at least, the existence of procedures guaranteeing that the service company does not have access to the data;
  - encryption of data transmissions (e.g.: HTTPS type connection, VPN, etc.);
  - guarantees in terms of network protection, traceability (logs, audits), access rights management, authentication, etc.
- **Sign a contract with the subcontractors**[33]**,** which defines the subject, the length and the purpose of the processing, as well as obligations of each party. Ensure that it contains, in particular, provisions targeting:
  - their obligation in terms of **confidentiality of the entrusted personal data;**
  - **minimal standards in terms of user authentication;**
  - **conditions of restitution of data and/or its destruction** at end of the contract;
  - **incident management and notification rules.** They should include notification of the data controller whenever a security breach or a security incident is discovered[34], which should happen as soon as possible when it concerns personal data.

WHAT SHOULD BE AVOIDED

- Starting the sub-contracting service without having signed a contract with the sub-contractor including the demands required by article 28 of the General Data Protection Regulation.
- Using cloud computing services in the absence of any guarantee regarding the effective geographical location of the data or without ensuring the lawfulness of the data transfers outside of the European Union and/or the necessity to obtain an authorization from the CNIL to proceed to the data transfer.

FURTHER MEASURES

- See article 28 of the General Data Protection Regulation.
- Regarding cloud computing, the CNIL has published recommendations, as well as proposals of clauses for contracts[35].
- Concerning health data, health data hosting services must receive an approval issued by the “ministère de la Santé” (Ministry for Health)[36]. The reference framework describing how to request such an approval is available on their website[37]. It is worth noting that a certification procedure will gradually replace the authorisation of hosting services (see Order n°. 2017-27 of 12th January 2017 relating to personal health data hosting).

33 The CNIL has published a subcontractor guide for this, available at the following address: https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
34 A security incident is characterised as a "personal data breach" when it affects personal data.
35 https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services
36 List accessible at http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees)
37 http://esante.gouv.fr/
38 https://www.legifrance.gouv.fr/eli/ordonnance/2017/1/12/2017-27/jo/texte

14

SECURING EXCHANGES WITH OTHER ORGANISATIONS

Strengthen the security of every personal data transmissions.

Electronic messaging services are not a secure means of communication to transmit personal data, without additional measures. A simple handling error can result in the disclosure of personal data to non-authorised recipients and therefore interfere with the persons' right to privacy. In addition, any entity with access to the messaging servers concerned (especially those of the senders and recipients) can have access to their content.

BASIC PRECAUTIONS

- **Encrypt the data before sending it on a physical medium** (DVD, USB stick, portable hard drive) to a third **party.**
- **When sending data through network:**
  - **encrypt** sensitive **documents** before sending them, if this transmission uses electronic messaging. Regarding this subject, it is advisable to refer to the recommendations of *factsheet n°. 17 - Using cryptographic functions*;
  - use a protocol guaranteeing the confidentiality and authentication of the recipient server for file transfers, for example **SFTP** or **HTTPS,** by using **the most recent version of protocols.**
  - **ensure the confidentiality of secrets** (encryption keys, passwords, etc.) by sending them via a separate channel (for example, sending an encrypted file by email and communicating the password by phone or SMS).
- If you need to use **a fax,** set up the following measures:
  - install the fax in a location only accessible to authorised personnel with physical access controls ;
  - display the identity of the receiving machine when sending messages;
  - 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

- Transmitting files containing unencrypted personal data via general public email providers.

FURTHER MEASURES

- The use of public key algorithms, when the different stakeholders have set up a **public key infrastructure,** seems particularly suitable to guarantee the confidentiality and integrity of the communications, as well as the authentication of the sender.
- The sender can **electronically sign the data** before sending it to guarantee that he or she is the source of the transmission (see *Factsheet n°. 17*).

15

PHYSICAL SECURITY

Strengthen the security of the premises housing IT servers and network equipment.

Access to the premises must be controlled to avoid or slow down unauthorised access, whether it is to paper files or IT equipments, especially servers.

BASIC PRECAUTIONS

- Install **anti-intrusion alarms** and check them periodically.
- **Set up smoke detectors, as well as firefighting resources,** and inspect them annually.
- Ensure the security of the keys and alarm codes granting access to the premises.
- **Separate areas of the building according to risks** (for example using a dedicated access control for the computer room).
- Keep an up-to-date list of the individuals or categories of individuals authorised to enter each area.
- **Establish the rules and methods for controlling visitor access,** at a minimum by having **visitors accompanie, outside of the public reception areas**[39] by a person from your organisation.
- Physically protect the IT equipment via specific methods (dedicated fire prevention system, raising equipments against possible floods, electrical supply and/or air conditioning redundancy, etc.).

WHAT SHOULD BE AVOIDED

- Undersizing or overlooking the maintenance of the computer rooms (air conditioning, UPS, etc.). A failure of these systems often results in machines stopping to work or in the opening of access to the rooms (air circulation) which neutralise elements contributing to the physical security of the premises.

FURTHER MEASURES

- Keep an access log of the rooms or offices likely to house equipment containing personal data that could have a serious negative impact on data subjects. **Inform users** of the installation of such a system, after informing and consulting with personnel representatives.
- Ensure that only authorised personnel are admitted into the restricted access areas. For example:
  - inside of controlled access areas, require all individuals to **wear a visible identification** (badge);
  - visitors (personnel in charge of technical assistance, etc.) must have a limited access. The date and time of their arrival and departure must be recorded;
  - reassess and regularly update the access permissions to secured areas and remove them if required.

39 From their entrance, throughout their visit and until they leave the premises.

16

SUPERVISING SOFTWARE DEVELOPMENT

Integrate security and privacy as early as possible into projects.

Privacy must be integrated into software development from the design stages, in order to offer data subjects a better control over their data and limit errors, losses, unauthorised modifications, or wrongful use of personal data in applications.

BASIC PRECAUTIONS

- **Integrate privacy, including its security requirements, from the design** of applications or services. These requirements can influence choices of architecture (decentralised vs centralised), features (fast anonymisation, data minimisation), technologies (encryption), etc.
- **For any development for the general public, examine the parameters relating to privacy,** and especially their default configuration.
- **Avoid free text inputs or comment zones.**
- Carry out software development and tests in a computing environment separated from the production (for example, on different computers or virtual machines) and use fictional or anonymised data.

WHAT SHOULD BE AVOIDED

- Using actual personal data in development and testing stages. Fictional sets should be used whenever possible.
- Developing applications or services without taking into account security.

FURTHER MEASURES

- Development must require **data acquisition and recording formats that minimize the collection of data.** For example, if only the year of birth of a person is necessary, the corresponding form should not allow to input 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 retention period chosen. For example, if a digital document must be kept for 20 years, it could be relevant to favour open standards that are more likely to be maintained in the long term.
- The creation and management of user profiles granting access rights to data depending on the user profile must be integrated from the development stages.
- An article dedicated to free text inputs and comment zones is accessible on our CNIL website[40].
- Depending on the application, it may be necessary to ensure its integrity with signatures of executable code to guarantee that it has not undergone any alteration.

17

ENCRYPTING, GUARANTEEING INTEGRITY AND SIGNING

Ensure the integrity, confidentiality and authenticity of a piece of information.

Hash functions are able to ensure the **integrity of data. Digital signatures,** in addition to ensuring the integrity, are able to verify the origin of the information and its **authenticity.** Finally, **encryption** makes it possible to guarantee the **confidentiality** of a message.

BASIC PRECAUTIONS

- **Use a recognised and secure algorithm,** for example, the following algorithms:
  - SHA-256, SHA-512 or SHA-3[41] as a hash function;
  - HMAC using SHA-256, bcrypt, scrypt or PBKDF2 to store passwords;
  - AES or AES-CBC for symmetric encryption;
  - RSA-OAEP as defined in PKCS#1 v2.1 for asymmetric encryption;
  - finally, for signatures, RSA-SSA-PSS as specified in PKCS#1 v2.1.
- **Use appropriate key sizes[42],** for AES it is advisable to use keys of 128 bits and, for algorithms based on RSA, modules and secret exponents of at least 2048 bits or 3072 bits, with public exponents, for encryption, greater than 65536.
- **Protect secret keys** by, at least, restrictive access rights and a secure password.
- **Create a procedure describing how to manage keys and certificates** taking into account the case of forgotten passwords.

WHAT SHOULD BE AVOIDED

- Using obsolete algorithms, like DES and 3DES for encryption or MD5 and SHA1 as hash functions.
- Confusing a hash function and an encryption algorithm, or considering that a hash function on its own is enough to ensure data confidentiality. Although hash functions are "one-way" functions, in other words functions that are difficult to reverse, data can sometimes be recovered from its hash. These functions are, by design, quick to use, thus it is usually possible to automatically hash all possible inputs and therefore to recognise the output.

FURTHER MEASURES

- "Comprendre les grands principes de la cryptologie et du chiffrement" (Understanding the main principles of cryptology and encryption) accessible at the following address: https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement.
- When an electronic certificate is received, **check that the certificate** usage is consistent with what is expected, that it **is valid and not revoked and that it has a correct certification chain** on all levels.
- **Use software or cryptographic libraries that have been audited by third parties with proven expertise.**
- Different encryption solutions can be used, such as:
  - solutions certified or qualified by the ANSSI[43];
  - the VeraCrypt software, allowing for the implementation of encrypted[44] containers;
  - the GNU Privacy Guard software, allowing for the establishment of asymmetric cryptography (signature and encryption)[45].

41 SHA-256 as defined in the FIPS 180-2.
42 A state of the art is available in the appendices of the "Référentiel Général de Sécurité" published by the ANSSI on its website.
43 https://www.ssi.gouv.fr/entreprise/ in the certification and qualification sections.
44 Container is a directory likely to contain several directories.
45 https://www.gnupg.org/index.fr.html

ASSESS THE SECURITY LEVEL OF THE PERSONAL DATA IN YOUR ORGANISATION

Have you considered...?

FACTSHEET		MEASURE	
1	Raising user awareness	Inform and raise awareness among individuals handling data	☐
		Write an IT charter and enforce its application	☐
2	Authenticating	Define a unique identifier (login) for each user	☐
		Adopt a user password policy conform to our recommendations	☐
		Require each user to change his or her password whenever it has been resetted	☐
		Limit the number of access attempts to an account	☐
3	Access Management	Define authorisation profiles	☐
		Remove obsolete access permissions	☐
		Carry out an annual review of authorisations	☐
4	Logging access and managing incidents	Implement a logging system	☐
		Inform users of the implementation of the logging system	☐
		Protect logging equipment and the information logged	☐
		Organise the procedures for personal data breach notifications	☐
5	Securing workstations	Organise an automatic session locking procedure	☐
		Use regularly updated antivirus software	☐
		Install firewall software	☐
		Collect the user's consent before any intervention on his or her workstation	☐
6	Securing mobile data processing	Organise encryption measures for mobile equipment	☐
		Undertake regular data backups and synchronisations	☐
		Require a confidential piece of information to unlock smartphones	☐
7	Protecting the internal network	Limit the network traffic to the bare essentials	☐
		Secure remote access to mobile computing devices via VPN	☐
		Implement the WPA2 or WPA2-PSK protocol for Wi-Fi networks	☐
8	Securing servers	Allow access to tools and administration interface only to qualified individuals	☐
		Install critical updates without delay	☐
		Ensure availability of data	☐
9	Securing websites	Use the TLS protocol and check its implementation	☐
		Check that no password or identifier are transferred via URLs	☐
		Check that the user inputs correspond to what is expected	☐
		Place a consent banner for cookies not required by the service	☐
10	Ensuring continuity	Carry out regular backups	☐
		Store the backup media in a secure place	☐
		Organise security measures for the transport of backups	☐
		Organise and regularly test the business continuity	☐
11	Archiving securely	Implement specific access methods to archived data	☐
		Destroy obsolete archives securely	☐
12	Supervising maintenance and data destruction	Record maintenance in a register	☐
		Have a responsible person from the organisation supervise work by third parties	☐
		Delete the data from all hardware before it is discarded	☐
13	Managing dataprocessors	Add a specific clause in the contracts of subcontractors	☐
		Organise the restitution and destruction conditions of data	☐
		Ensure the effectiveness of provided guarantees (security audits, visits, etc.)	☐
14	Securing exchanges with other organisations	Encrypt data before sending it	☐
		Ensure that it is the right recipient	☐
		Send the secret information separately and via a different channel	☐
15	Physical security	Restrict access to the premises via locked doors	☐
		Install anti-intrusion alarms and check them periodically	☐
16	Supervising software development	Offer parameters that respect the privacy of end users	☐
		Avoid comment zones or supervise them strictly	☐
		Carry out tests on fictional or anonymised data	☐
17	Using cryptographic functions	Use recognised algorithms, software and libraries	☐
		Keep the secret information and cryptographic keys in a secure way	☐