



PRACTICE GUIDE GDPR

**SECURITY OF
PERSONAL DATA**
Version 2024

The objective of this guide is to support organisations in the implementation of security measures in order to ensure the protection of personal data that they treat.

It is aimed in particular at data protection officers (DPO), chief information security officer (CISO) and computer scientists. Privacy lawyers will also be able to find useful elements.

This guide is a living tool that is enriched by state-of-the-art practices and doctrine elements of the French data protection authority (CNIL) on the issue of data security.

A changelog is available on the CNIL website to help actors identify the evolutions that need to be taken into account in order to adapt their level of security.

	FOREWORD	4
FACTSHEET 1	Managing data security	5
	 USERS	
FACTSHEET 2	Defining a framework for users	9
FACTSHEET 3	Involving and training users	11
FACTSHEET 4	Authenticating users	13
FACTSHEET 5	Access management	16
	 MY INFORMATION TECHNOLOGY AND MY EQUIPMENTS	
FACTSHEET 6	Securing workstations	18
FACTSHEET 7	Securing mobile computing	20
FACTSHEET 8	Protecting the computer network	22
FACTSHEET 9	Securing servers	24
FACTSHEET 10	Securing websites	26
FACTSHEET 11	Managing IT developments	28
FACTSHEET 12	Protecting the premises	30
	 MY CONTROL OVER DATA	
FACTSHEET 13	Securing exchanges with the outside world	33
FACTSHEET 14	Managing data processors	35
FACTSHEET 15	Supervising the maintenance and end-of-life of hardware and software	37
	 PREPARING FOR AN INCIDENT	
FACTSHEET 16	Logging operations	40
FACTSHEET 17	Saving	42
FACTSHEET 18	Predicting continuity and resumption of activity	43
FACTSHEET 19	Managing incidents and violations	44
	 FOCUS	
FACTSHEET 20	Risk analysis	47
FACTSHEET 21	Encryption, hash, signature	50
FACTSHEET 22	Cloud computing	52
FACTSHEET 23	Mobile applications: Design and development	54
FACTSHEET 24	Artificial intelligence: Design and learning	56
FACTSHEET 25	API: Application programming interfaces	58
	ASSESS THE SECURITY LEVEL OF MY ORGANISATION'S PERSONAL DATA	60

FOREWORD

Security is an essential part of the protection of personal data. It is binding on any data controller and data processor through Article 32 of the General Data Protection Regulation¹ (GDPR). In principle, each processing operation must be subjected to a set of security measures decided according to the context, namely **“useful precautions, having regard to the nature of the data and the risks presented by the processing”** (Article 121 of the French Data Protection Act²). The GDPR specifies that the protection of personal data requires taking *“appropriate technical and organisational measures to ensure a **level of security appropriate to the risk**”* for the rights and freedoms of natural persons, including their privacy.

To assess the measures to be put in place, two complementary approaches are to be deployed:

- the establishment of a security base incorporating good practices resulting from years of capitalising on hygiene and IT security (e.g.: regulations, standards, guides). This base aims to address the most common risks;
- the risk analysis³ for the persons concerned by the processing, which aims to identify and assess the risks specific to the treatment. Such an analysis supports objective decision-making on the treatment of these risks and the identification of necessary and context-appropriate measures.

However, it is difficult for non-specialists in IT security to implement such an approach and to ensure that the level of security of the processing for which they are responsible is sufficient.

To help with compliance, this guide presents a set of recommendations grouped by thematic factsheets. Each factsheet is structured in three sections:

- basic precautions, which incorporate essential good practices;
- bad trend practices, which should be avoided;
- additional measures, to go further⁴.

Each factsheet can be read separately from the others: references are given when another factsheet.

¹ “The General Data Protection Regulation – GDPR”, eur-lex.europa.eu

² “La loi Informatique et Libertés”, cnil.fr

³ In particular, it is essential when the processing has to be subject to a data protection impact assessment or DPIA (see “Ce qu’il faut savoir sur l’analyse d’impact relative à la protection des données (AIPD)”, cnil.fr).

⁴ These measures may over time and practice become basic precautions.

FACTSHEET 1 – MANAGING DATA SECURITY

Implement and maintain the protection of personal data required by the GDPR and sectoral frameworks.

The integration of data protection into the decision-making processes of the organisation ensures that it is taken into account over time and at key moments when budgets and projects are decided.

Basic precautions

- **Involve the management** and formalise general objectives in terms of security and protection of personal data, approved by the organisation's management.
- **Identify** (through the register⁵) **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 systems, business software);
 - the cloud computing resources used (e.g.: SaaS, PaaS, IaaS);
 - the logical or physical communication channels (e.g.: wired connections, Wi-Fi, Internet, verbal exchanges, couriers);
 - the paper documents (e.g.: printed documents, photocopies);
 - the physical premises and facilities where the above-mentioned elements are located (e.g.: IT rooms, offices).

Formalise interconnecting and data flow diagrams between the different components of information systems. The register and diagrams must be updated whenever there is structural change to the processing or components of the information systems.

- **Define an IT security action plan and implement the technical and organisational measures defined** to ensure data protection. To this end, two complementary approaches can be implemented: on the one hand, implementing the basic precautions listed in this guide (see the assessment checklist) and, on the other hand, supplementing these with specific measures identified using risk analysis⁶ (see [factsheet 20 – Risk analysis](#)).

Any new measures decided must incorporate the action plan, the progress of which is monitored on a regular basis.

- **Periodically check the effectiveness of technical and organisational measures** to ensure that they are achieving their intended purpose (e.g. by setting up indicators). Prioritise the measures implemented to address identified vulnerabilities or to prevent incidents that have already occurred.
- **Ensure that management is kept informed** of IT risk management through a management review at least once a year. It should enable decision to be taken and summary to be produced a summary to be produced and decisions to be taken bearing in mind:
 - the changing context, challenges and expectations of stakeholders (e.g.: customers, partners, supervisory authorities);
 - the changing objectives and missions of the organisation;
 - the evolution of cyber threats;
 - the development of new security technologies or solutions;

⁵ "Le registre des activités de traitement", cnil.fr

⁶ Article 35 of the GDPR requires a data protection impact assessment (DPIA) for certain types of processing (see "Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)", cnil.fr).

- the evolving nature of information systems and data processing;
 - the evolution of data security and privacy risks;
 - the progress made on the legal action plan (e.g.: compliance of contracts) and the technical action plan (security measures);
 - the incidents and breaches encountered, with their impact on the organisation and the data subject;
 - the requests and complaints received and processed concerning personal data.
- **Improve the protection of personal data over time.** In particular, the management review should make it possible to decide on the allocation of the human and budgetary resources needed for the measures to be put in place and for the continuous improvement of security.

What should be avoided

- Considering security as an afterthought that can be dealt with at a later stage, once data processing is already operational.
- Focusing on advanced measures without having in place the basic precautions.
- Being limited to one-off actions and not considering data processing as a whole (e.g. data collection, partners, end-of-life) when deciding on security measures to be put in place.
- Relying solely on technical measures without backing them up with coherent organisational measures.
- Defining an action plan without assigning a deadline and responsible for implementation to each action.
- Delegating the management of all IT security to a provider.

- For day-to-day monitoring of security and data protection, it is very useful (or even mandatory depending on the nature of the organisation) **to appoint a chief information security officer (CISO) and a data protection officer⁷ (DPO)**. They must:
 - be qualified to **report directly to the highest level of management**;
 - **have the necessary resources and working conditions** to carry out their duties;
 - **be involved** (themselves own or their team) systematically and at an early stage in the discussions on issues relating to their area of responsibilities, in order to ensure that information systems are secured and the personal data are protected **by design and by default**.
- The general objectives for the protection of personal data can be recorded in a general data protection policy, endorsed by management and communicated to all those involved (staff, subcontractors, partners). This policy can then be specified at an operational level in the form of thematic policies and detailed procedures to adapt the measures for the protection of personal data to the context of the organisation's activities.
- **Security audits are an essential means of assessing the level of security of the systems on which the processing of personal data is based.** Carried out periodically, they allow taking changes in processing and threats into account. Each audit must produce an action plan, the implementation of which should be monitored at the highest level of the organisation.
- In order to structure governance over time, it is possible to set up a management system based on a continuous improvement approach. The International Standard ISO/IEC 27701⁸ describes the organisational and technical processes and measures to implement a Privacy Information Management System (PIMS), based on the Information Security Management System (ISMS) covered by Standard ISO/IEC 27001.
- The French National Cybersecurity Agency (ANSSI) has published its own guide⁹ on best practices in IT security.

⁷ "Devenir délégué à la protection des données", cnil.fr

⁸ "L'ISO 27701, une norme internationale pour la protection des données personnelles", cnil.fr

⁹ "Guideline for a healthy information system in 42 measures", cyber.gouv.fr

USERS

FACTSHEET 2 – DEFINING A FRAMEWORK FOR USERS

Give binding force to the main rules for the use of IT tools.

Users often have daily use of the IT tools. Their practices can have a direct impact on the security of personal data and therefore need to be framed.

Basic precautions

- **Draft an IT charter and give it binding force** (e.g.: annexation to the Rules of Procedure).
- **Include in the charter** at least the following:
 1. A reminder of the rules of data protection and of the sanctions incurred for non-compliance with these rules.
 2. The scope of the application of the charter, which should include in particular:
 - the methods of intervention of the teams responsible for managing the organisation's IT resources;
 - the authentication methods used by the organisation and the password policy that the user must respect;
 - the security rules that users must comply with including:
 - reporting to the internal IT department any suspected breach or attempt to breach its computer account, any loss or theft of equipment and, in general, any malfunction;
 - never entrusting your password (or equivalent) to a third party;
 - never installing, copying, modifying, destroying or configuring software without permission;
 - locking (or turning off) your computer as soon as you leave your workstation;
 - not accessing, attempting to access or delete information if this is not the responsibility of the user;
 - respecting the procedures previously defined by the organisation in order to regulate the operations of copying data on removable media, in particular by obtaining the prior approval of the hierarchical superior and by complying with the security rules.
 3. The procedures for the use of IT equipment and telecommunications resources made available such as:
 - workstations;
 - mobile equipment (especially in the context of teleworking);
 - individual storage spaces;
 - local networks;
 - personal devices (especially the conditions to use such devices);
 - the Internet;
 - electronic messaging;
 - telephony.
 4. The conditions governing the administration of the information system, and the existence, where applicable, of:
 - automatic filtering systems;
 - automatic logging systems;
 - workstation management systems.
 5. The responsibilities and sanctions incurred in the event of non-compliance with the charter.

What should be avoided

- Not giving binding force to the charter or not applying and enforcing it in case of non-compliance.
- Not considering the real practices of users, their expectations and their needs by defining the rules for the use of IT means: shadow IT sometimes reveals essential needs that are not met by the organisation or a structural malfunction.
- Not supporting users in their practices.

TO GO FURTHER

- Provide for the signature **of a confidentiality commitment** (see example clause below), or include in employment contracts a **specific confidentiality clause** concerning personal data.
- Provide for a specific charter for administrators which details the additional requirements that this particularly at-risk population must comply with.

Example of a confidentiality commitment clause for individuals who are intended to manipulate personal data

I, the undersigned Mr/Mrs. exercising the functions of _____ within the company _____ (hereinafter referred to as "the Company"), being therefore required to access personal data, declares that I recognise the confidentiality of such data.

I therefore undertake, in accordance with Article 32 of the General Data Protection Regulation of 27 April 2016, to take all precautions in accordance with the state of the art and internal rules within the framework of my powers in order to protect the confidentiality of the information to which I have access, and in particular to prevent it from being communicated to persons not expressly authorised to receive such information.

In particular, I undertake to:

- not to use the data that I can access for purposes other than those provided for by my powers;
- disclose this data only to persons duly authorised, by reason of their functions, to receive such information, whether private, public, natural or legal;
- not to make any copies of this data except as necessary for the performance of my duties;
- take all measures consistent with the state of the art and internal rules within the framework of my powers in order to avoid the misuse or fraudulent use of this data;
- take all precautions in accordance with the state of the art and internal rules to preserve the physical and logical security of this data;
- ensure, within my powers, that only secure means of communication will be used to transfer this data;
- in the event of termination of my duties, return in full the data, computer files and any information media relating to these data.

This confidentiality commitment, in force for the duration of my duties, will remain effective, after the termination of my duties, whatever the cause and until the data has been made public by the Company, provided that this commitment concerns the use and communication of personal data.

I have been informed that any breach of this undertaking exposes me to disciplinary and criminal sanctions in accordance with the regulations in force, in particular with regard to Articles 226-13 and 226-16 to 226-24 of the Criminal Code.

Done at xxx, xxx, in xxx copies

Name:

Signature:

FACTSHEET 3 – INVOLVING AND TRAINING USERS

Make each user aware of privacy and security challenges.

Human errors and social engineering attacks are responsible for a significant number of security incidents. Technical solutions are not sufficient to ensure the protection of personal data held by organisations.

Basic precautions

- **Raise awareness among users (both internal and external to the organisation) working with personal data about the privacy risks, informing them of** the measures implemented to address these risks and the potential consequences in case of non-compliance. Concretely, it can be:
 - organise awareness sessions on risks, the main types of attacks (e.g.: phishing, ransomware, identity theft), the necessary vigilance (e.g.: before opening an attachment or clicking on a link in a message, when answering the phone), and what to do in the event of an incident or suspicion (protection and warning measures);
 - regularly send instructions reminders according to the current events of the organisation (e.g.: recent phishing attempt, arrival of a new provider).
- Deploy different awareness campaigns whose **content and language are adapted to the roles of the recipients**. For example, human resources staff need to be made aware of the data they handle, and the employees who work off-site need to be made aware of the specific risks of nomadism.
- Ensure that staff in charge of processing personal data (e.g.: those in charge of handling complaints or administrative documents) have fully assimilated good practices relating to the protection of personal data to be implemented on a daily basis (e.g.: knowledge assessment).
- Train staff in charge of IT tools (e.g.: those in charge of design and maintenance) in IT security and protection of personal data.
- **Document the operating procedures**, keep them up to date and make them available to all users concerned. In concrete terms, any action on personal data, whether it is an administration-related operations or plain use of an application, must be explained in clear language adapted to each category, in documents to which the users can refer.

What should be avoided

- Imposing IT tools without accompanying their adoption by the teams.
- Not making it mandatory for new recruits to attend to session on the protection of personal data, when the organisation's main activity involve processing of personal data (e.g.: health facility, customer service).
- Underestimating the positive impact that well-informed employees can have on the organisation's IT security.
- Not ensuring the awareness of external service providers (by direct action or by contractual commitment) when their impact on data security can be just as significant as that of internal employees.

TO GO FURTHER

- Implement an **information classification** policy and tools defining several levels (e.g.: public, internal, confidential) and requiring to mark the documents, media and e-mails containing confidential data.
- Place a visible and explicit notice on each page of paper or electronic documents which contain sensitive data¹⁰.
- Organise **exercises and simulations of IT security incidents** or crises (with the prior organisation and supervision required for any security exercise). These exercises enable to review how well the instructions have been applied and the effectiveness of incident and crisis management procedures in place. Consolidating the feedback from these exercises enable to identify the messages to be strengthened and the procedures to be improved.

¹⁰ Sensitive data are described in Article 6 of the French Data Protection and Freedoms Act and Article 9 of the GDPR.

FACTSHEET 4 – AUTHENTICATING USERS

Recognising users so that they can be given the necessary accesses.

Before any use of IT resources, a user must be given an **identifier of his own and must authenticate himself** so that his identity and accesses to the data he needs can be checked.

The mechanisms for carrying out the authentication of persons are categorised according to whether they involve:

- a knowledge factor (what one knows), e.g. a password;
- a possession factor (what one has), for example a smart card;
- an inherent factor (what one is), for example a fingerprint or keystroke dynamics¹¹. As a reminder, the processing of biometric data for the purpose of uniquely identifying a natural person on the basis of his physical, physiological or behavioural characteristics is a processing of sensitive data which gives rise to the application of Article 9 of the GDPR¹².

User authentication is defined as **multi-factor** when it uses a **combination of at least two factors** of distinct categories. It is referred to as **strong** if it is based on a cryptographic mechanism whose parameters and security are considered robust (e.g.: cryptographic key).

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 a hierarchy validation, implement measures to log the actions associated with these identifiers and renew the password as soon as a person no longer needs to access the account.
- **Respect the CNIL recommendation¹³ in the case of password-based user authentication**, notably by applying the following rules:
 - store only the fingerprints of passwords, obtained using state-of-the-art techniques;
 - do not request a periodic renewal of passwords for simple users (unlike administrators);
 - when he or she first logs in, require the user to change any password attributed automatically or by an administrator when creating the account or resetting the password;
 - impose password complexity according to the use cases:
 - **by default, entropy¹⁴** (theoretical unpredictability) **minimum of 80 bits** (e.g.: Minimum 12 characters with uppercases, lowercases, digits and special characters; Minimum 14 characters with uppercases, lowercases and digits, with no mandatory special character);
 - 50-bit entropy (e.g.: Minimum 8 characters of 3 different types; 16 digits) in case additional measures are in place (restriction of access to the account such as delaying access after several failures, setting up “Captcha” or blocking the account after 10 failures);
 - 13-bit entropy (e.g.: 4 digits) in the case of equipment owned by the user (e.g.: SIM card, device containing a certificate) with blocking after 3 failures.

¹¹ Behavioral biometrics (e.g.: keystroke dynamics) is less mature than physiological biometrics (e.g.: fingerprint scans).

¹² For workplace authentication, any controller wishing to carry out such processing must comply with the requirements of the regulatory framework on access by biometric authentication in the workplace (see “Le contrôle d’accès sur les lieux de travail”, cnil.fr).

¹³ “Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité”, cnil.fr

¹⁴ Entropy, applied to a password, corresponds to its ability to resist a brute force attack.

For example, for the secret code of a credit card, the number of possible combinations is equal to 10 (possible figures) to the power 4 (104). In binary, to obtain an equivalent number of combinations, it is necessary to use 13 bits, because 2 (possible bits) at the power 13 (213) is worth 8192, which is of the same order of magnitude as 10 4. This gives an entropy of 13 bits.

- **Support users in choosing a strong password:**
 - by raising awareness of **mnemonic methods**¹⁵;
 - by encouraging the use of **password managers**¹⁶ and providing training in their use:
 - it enables to securely register as many passwords as necessary while requiring only one master password to be memorised;
 - the master password must therefore be particularly strong;
 - particular attention must be paid to the choice of solution.
- **Communicate on prohibited practices**¹⁷ (e.g.: communicating your password to anyone else, using a password that can be deduced from the context in which it is used, save passwords in a browser without a master password). **In case of bad practices, a password respecting the required entropy can always be easily used by an attacker.**

What should be avoided

- Using the default passwords of equipment and software.
- Storing passwords in clear text, not as a cryptographic fingerprint.
- Using an obsolete cryptographic hash function, such as MD5 or SHA-1 ([see factsheet 21 – Encryption, hash, signature](#)) for generating the password footprint to be stored, or designed internally, which is therefore unrecognised or proven.
- Preventing the use of the “Paste” or auto-complete function in forms to avoid impacting the use of a password manager.

¹⁵ “Générer un mot de passe solide”, cnil.fr

¹⁶ “5 arguments pour adopter le gestionnaire de mots de passe”, cnil.fr

¹⁷ “Les conseils de la CNIL pour un bon mot de passe”, cnil.fr

TO GO FURTHER

- **Favour multi-factor authentication** whenever possible, especially when the connection is accessible from outside the organisation's network.
- **Limit the number of access attempts** to user accounts on workstations and block access to the account temporarily or not, when its limit is reached.
- **Require administrators to use higher entropy passwords and renew them on a reasonable and relevant frequency.**
- Implement technical measures to **enforce authentication rules** (e.g.: blocking an administrator's account if a password is not updated).
- On its website, the CNIL provides a tool¹⁸ for calculating the complexity of passwords requested from users, depending on each use case (password alone, with access restrictions or with material held by the person).
- If possible, avoid making the identifiers (or logins) of users and administrators the same as accounts defined by default by the software companies and deactivate default accounts.
- **Store passwords securely**, processed with a function (hash) specifically designed for this purpose and always using a salt or key¹⁹ ([see factsheet 21 – Encryption, hash, signature](#)). A key must not be stored in the same database as the fingerprints of the passwords.
- The ANSSI in collaboration with the CNIL²⁰, published recommendations on multi-factor authentication and passwords. Also refer to the guides²¹ published by the ANSSI to help developers and administrators in their choice of cryptographic algorithms, sizing and implementation.
- For administrative authorities, the Annexes to the "*référentiel général de sécurité*" (RGS²²) apply, in particular annexes B1 and B2 concerning cryptographic mechanisms and key management, respectively.

18 "Vérifier sa politique de mots de passe", [cnil.fr](#)

19 The random used is called "salt" when it is different for each password stored and "key" when it is common to the transformation of a set of passwords (e.g. for a whole database).

20 "Recommandations relatives à l'authentification multifacteurs et aux mots de passe", [cyber.gouv.fr](#)

21 "Mécanismes cryptographiques", [cyber.gouv.fr](#)

22 "Le référentiel général de sécurité version 2.0: documents", [cyber.gouv.fr](#)

FACTSHEET 5 – ACCESS MANAGEMENT

Only allow access to data that the user really needs.

Respecting the principle of least privilege, through the management of the authorisation profiles, allows to limit the consequences of an account usurpation or an error of manipulation.

Basic precautions

- **Define authorisation profiles** in systems by separating tasks and areas of responsibility, in order to restrict users' access to only the data strictly necessary for fulfilling their responsibilities.
- **Get all request for authorisation validated** by a manager (e.g.: line manager, project manager).
- **Withdraw users' access right as soon as they are no longer authorised to access a room or an IT resource** (e.g. change of mission or post) **as well as at the end of their contract.**
- **Carry out a regular review, at least annually, of authorisations in order** to identify and delete unused accounts and realign the rights granted to each user's responsibilities. The business managers should be involved in this review so that they can ensure the operational legitimacy of the rights granted.

What should be avoided

- Creating or using accounts shared by several people without tracing these exceptions to the security rules, without having them validated by the appropriate managers and without regularly reviewing them.
- 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 (e.g.: for a replacement).
- Forgetting to delete user accounts of people who have left the organisation or changed their functions.

TO GO FURTHER

- Establish, document and regularly review **an access control policy** in relation to the processing operations implemented by the organisation, which must include:
 - the procedures to be applied automatically upon arrival and departure or 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 (e.g.: misuse of a right of legitimate access);
 - the measures allowing to restrict and control the granting and use of access to processing ([see factsheet 16 – Logging operations](#)).

MY INFORMATION TECHNOLOGY AND MY EQUIPMENTS

FACTSHEET 6 – SECURING WORKSTATIONS

Prevent fraudulent access, malicious programs execution (e.g.: virus) or remote control, including via the Internet.

There is an abundance of IT intrusion risks and workstations embody one of the key entry points.

Basic precautions

- Provide an **automatic session locking** mechanism triggered whenever the workstation has not been in use for a given time.
- Install a **firewall** software on the station and restrict the opening of communication ports to those strictly necessary to the applications installed on the workstation for proper running.
- Use **regularly updated antivirus**.
- **Patch security breaches with appropriated security updates as soon as possible** after testing them. Updates patching publicly disclosed critical flaws must be installed with no delay.
- Keep users' rights to the strict minimum based on their needs for their workstations' use.
- **Enable and promote the storage of users' data on a regularly backed up online storage space accessible through the organisation's internal network** rather than on the actual workstations. If data is locally stored, provide synchronisation or backup means to users and train them to use them.
- **Securely erase data on any workstation before reassigning it** to another person.
- Regarding removable supports (e.g.: USB sticks, external hard drives):
 - raise the users' awareness about removable devices' associated risks, especially if they come from the outside;
 - **restrict the connection of removable media** to the strictly necessary;
 - disable "autorun" from removable media.
- For **assistance on workstations**:
 - remote administration tools must **obtain consent** from the user prior to any intervention on his/her position (e.g.: whenever an appointment was agreed upon, by displaying a message to the user that they have to agree to);
 - the user must also be able to **distinguish between whether the remote control is still in progress** and whether it ended (e.g.: by displaying a message on the screen).

What should be avoided

- Using obsolete operating systems whose support is no longer provided by the publisher.
- Provide administration privileges, both locally and on the network, to users whose position does not requires it (e.g.: administrators).

TO GO FURTHER

- **Only allow the execution of applications downloaded** from safe sources (white list).
- **Restrict the use** of applications requiring administrator rights for their execution.
- Provide a secure environment (e.g.: virtualised temporary environment) for carrying out necessary operations involving a particular risk (e.g.: navigation on an untrusted website).
- Set up a solution for analysing and **decontaminating removable media** before each use. ANSSI has published a guide²³ to help choosing these types of solutions.
- **Upon the compromise of a workstation, look for the source as well as any trace of intrusion** into the organisation's information system to detect the compromise of other elements.
- **Monitor the software and hardware used in the organisation's information system.** CERT-FR, the French government centre for monitoring in charge of alerting and responding to computer attacks, issues on its website²⁴ alerts and notices on vulnerabilities discovered in software and hardware. Whenever possible it also provides means to guard against them.
- Deploy **critical updates to operating systems without delay** (if applicable after testing them) by scheduling a weekly automatic check.
- Provide a functional updates policy.
- Fasten workstations to specific or difficult to move furniture (e.g.: use anti-theft cables).
- Make sure all users are well informed about **the action to be taken and the list of persons to be contacted in the event of a security incident or an unusual event** affecting the organisation's information and communication systems.
- Consult²⁵ the CERT-FR page on good reflexes in case of intrusion on an information system.

²³ "Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés)", cyber.gouv.fr

²⁴ "CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques", cert.ssi.gouv.fr

²⁵ "Les bons réflexes en cas d'intrusion sur un système d'information", cert.ssi.gouv.fr

FACTSHEET 7 – SECURING MOBILE COMPUTING

Anticipate the breach of data security outside your premises, including theft or loss of mobile equipment.

A wide variety of remote work practices, outside the organisations' premises, have risen (e.g.: travel, teleworking) as well as the use of personal equipment for work purposes resulting to specific risks increase, specifically with the use of laptops, USB sticks or smartphones: supervising such risks is crucial.

Basic precautions

- **Raise users' awareness regarding specific risks associated with the use of mobile IT tools** (e.g. equipment theft, connection to uncontrolled networks and equipment risks, in particular public equipment, use of personal equipment) and procedures to restrict them.
- **Provide access control** through appropriate authentication devices (e.g.: electronic certificate, smart card). All information flows should be encrypted (e.g. VPN for external access).
- Provide users with **shared storage spaces that are remotely accessible**. Encourage them to store all their data there in order to mitigate the damages caused by loss or theft of their devices.
- **Implement or integrate an encryption solution for nomadic or removable storage devices** (e.g.: laptop, USB drive, external hard drive, CD-R, DVD-RW) such as:
 - hard disk encryption (many operating systems support such a functionality);
 - file-by-file encryption;
 - encrypted containers creation (folder that can contain multiple files).
- **Regarding smartphones**, on top of the SIM card's PIN use, **enable the automatic locking of the terminal and require a secret to unlock it** (e.g.: password, pattern).
- **Make sure that users are given the proper contact details** of the employee in charge in case of loss or theft of their devices.
- **Assess and address the specific risks associated with personal equipment use by users** (bring your own device or BYOD) **and authorise them only regarding those identified risks**. Such devices that are uncontrolled by the organisation shall be accordingly restricted in accessing data and application with regards with their criticality. Make sure that the IT charter covers and formalise the responsibilities of everyone involved as well as the precautions that have to be followed ([see factsheet 2 – Defining a framework for users](#)).

What should be avoided

- Using default cloud services installed by default on a device for backup or synchronization purposes without an in-depth analysis of their terms of use and security requirements complied by those services providers. These do not generally comply with the recommendations given in [factsheet 14 – Managing data processors](#).
- Enforcing security measures (e.g.: by restrictively setting up a mobile device management system, MDM, on a personal phone) that prevent the domestic use of personal equipment on the grounds that the device is used in a professional context (e.g. prohibit the installation of applications on the device).
- Breaking the user's privacy rights by accessing to data or elements stored in the user's personal storage space of their device used in
- Accessing elements relating to the privacy of persons stored in the personal space of personal

equipment used in the professional context (BYOD).

- See the factsheet dedicated²⁶ to the use of personal equipment by users on the CNIL website.
- **Set up a mobile device management system (MDM)**, including on personal devices used in the professional context (BYOD) if the practice is allowed, in order to standardise configurations and control the security assurance level of devices that connect to the organisation's network.
- **Provide a privacy filter** for workstations' screens if they are to be used in public spaces.
- Raise awareness on bad practices in public places:
 - **do not leave equipment or documents unattended;**
 - do not discuss (e.g.: group chat, phone calls) or share sensitive information (e.g.: personal data, information that may reveal security breaches).
- **Restrict local data storage** on nomadic workstations to what is strictly necessary, in particular for personal equipment, and possibly prohibit it when travelling abroad²⁷.
- **Protect yourself against theft** (e.g.: safety cable, visible marking of equipment) **and mitigate the impacts** (e.g.: automatic locking, encryption, remote deletion). If a deletion mechanism is to be used on a personal device (BYOD), the employer must incorporate its terms of use into the IT charter ([see factsheet 2 – Defining a framework for users](#)).
- Partition parts of personal equipment intended to be used in a professional setting.

²⁶ "BYOD : quelles sont les bonnes pratiques ?", cnil.fr

²⁷ "Best Practices For Business Travellers", cyber.gouv.fr

FACTSHEET 8 – PROTECTING THE COMPUTER NETWORK

Confine network functions to the extent strictly necessary for the execution of your processing.

Internal network interconnects all components of an organisation's information systems and often offers connection points with the outside. It is just as much an entry point as a medium for attacks propagation. Therefore, securing the internal network is critical.

Basic precautions

- **Limit Internet access** by blocking unnecessary services (e.g. VoIP, peer to peer).
- **Manage Wi-Fi networks.** They must use state-of-the-art encryption (WPA3 or WPA2 in accordance with ANSSI's configuration recommendations²⁸). Additionally, networks open to guests must be separated from the internal network.
- **Enforce VPN use for remote access** implementing, if possible, strong user authentication (e.g.: smart card, time-based one-time password (TOTP)).
- **Ensure that no administration interface is directly over the Internet.** Operations for administration and maintenance must be carried out through a VPN.
- For network administration purposes, best practice is to (correctly) configure and implement the SSH protocol or physically access the equipment.
- **Limit network flows to what is strictly necessary** by filtering incoming/outgoing flows on equipment (e.g.: firewalls, proxy servers). For instance, if a web server is on a HTTPS-only mode, you should only allow incoming flows on that machine on port 443 and block all other ports.
- **Partition the network** to mitigate potential security breaches impacts. Implement at least two distinguished network areas: **an internal network where no Internet connection is allowed and a DMZ** (demilitarized zone) **accessible from the Internet**, separated by gateways.

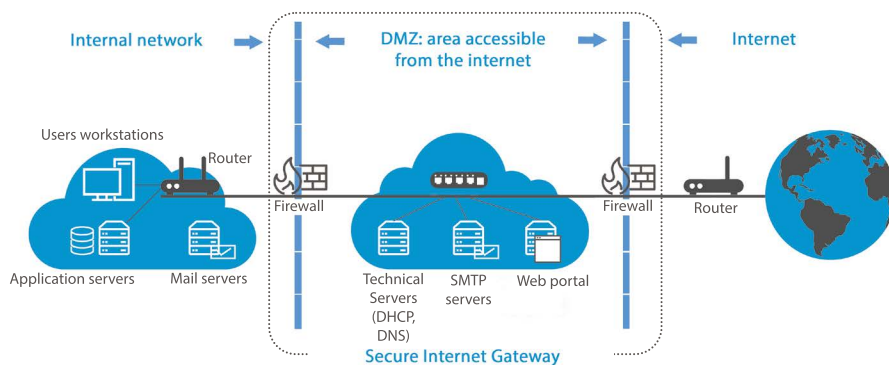
What should be avoided

- Using the Telnet protocol for active network equipment connection (e.g.: firewalls, routers, gateways).
- Providing users with unfiltered Internet access.
- Setting up a Wi-Fi network using WEP encryption.

²⁸ « Sécuriser les accès Wi-Fi », cyber.gouv.fr

TO GO FURTHER

- Administration and maintenance operations should be carried out from equipment under the exclusive control of the data controller or its subcontractors.
- **Automatic hardware identification can be implemented** by configuring hardware authentication (802.1X protocol) or, at least, by defining an updated identifiers whitelist of network interface controllers (MAC addresses) to restrain an unlisted device connection.
- **Intrusion Detection (IDS) and Intrusion Prevention (IPS) systems** can analyse network traffic to detect and even respond to some attacks. **Inform users** of the implementation of such systems in the IT charter ([see factsheet 2 – Defining a framework for users](#)), after informing and consulting staff union representatives.
- **ANSSI has published a good practices handbook**²⁹, to help decide for instance how to define the interface for connecting an information system to the Internet³⁰ (which are inspired by the diagram below), the choice of firewalls³¹ or the deployment of the 802.1X protocol³².



²⁹ "ANSSI's Publications", cyber.gouv.fr

³⁰ "Recommandations relatives à l'interconnexion d'un SI à Internet", cyber.gouv.fr

³¹ "Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet", cyber.gouv.fr

³² "Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux", cyber.gouv.fr

FACTSHEET 9 – SECURING SERVERS

Strengthen servers' security measures.

Since servers centralise a great amount of data as well as host services allowing to access to or manipulate said data, server security shall be a priority.

Basic precautions

- **Uninstall or disable unnecessary services and interfaces.**
- **Access to administration tools and interfaces shall be restricted to authorized personnel only.** Use user accounts without privileges for routine operations.
- **Adopt a specific password policy** for administrators. Change passwords, at least, during each departure of an administrator and in case of suspicion of compromise.
- **Install critical updates** without delay (if applicable after testing them), in particular security patches, whether for operating systems or applications, by scheduling a weekly automatic check-up.
- **Use malware detection and removal software** (e.g.: antivirus), update them regularly.
- **Use registered accounts** for databases access and create application-specific technical accounts.
- **Backup and regularly check backup files' integrity and the possibility to restore them** ([see factsheet 17 – Saving](#)).
- **Implement the TLS protocol** (instead of SSL³³), or a protocol ensuring encryption and authentication, at least for any exchange of data on the Internet and check its proper implementation by appropriate tools³⁴.
- Do not allow the use of outdated encryption algorithms for server communications.
- **Set up a logging event system** ([see factsheet 16 – Logging operations](#)).

What should be avoided

- Processing personal data on obsolete servers not replacing them.
- Using insecure data exchange protocols (e.g. unencrypted authentication, cleartext flows).
- Using servers for functions other than those they are dedicated to, such as browsing websites or accessing email.
- Placing databases on a server directly accessible from the Internet.
- Using generic accounts (i.e. shared between multiple users).

³³ The TLS protocol is sometimes wrongly called SSL or SSL/TLS. The SSL protocol, the predecessor of TLS, is now obsolete and to be banned.

³⁴ For TLS, there are several tools for this purpose (e.g.: "SSL Server Test", ssllabs.com, "SSL-Tools", ssl-tools.net).

TO GO FURTHER

- Any system processing sensitive data³⁵ must be implemented in a **dedicated environment** (logically isolated).
- **Server administration operations should be carried out through a dedicated and isolated network**, with strong authentication access ([see factsheet 5 – Access management](#)) for enhanced traceability ([see factsheet 16 – Logging operations](#)).
- In addition to external flows, **internal flows shall be encrypted** as much as possible (e.g. using TLS, IPsec or SSH protocols).
- Isolate obsolete but essential servers and limit the processing of personal data on it pending their replacement by up-to-date systems.
- As for software running on servers, use **vulnerability detection tools** (software of vulnerability scans such as nmap³⁶, nessus³⁷ or nikto³⁸) or rely on audits for the most critical processing to detect possible security vulnerabilities. Attacks detection and prevention systems on critical systems or servers can also be used.
- Restrict physical access and prohibit remote logical access to diagnosis and configuration ports.
- TLS v1.3 should be implemented and/or integrated or, at least, v1.2, in compliance to ANSSI's published recommendations on the subject³⁹.
- **ANSSI has published various**⁴⁰ **recommendations**, including securing the administration of information systems⁴¹ and setting up system partitioning⁴².

³⁵ Sensitive data are described in Article 6 of the Data Protection Act and Article 9 of the GDPR.

³⁶ "Nmap", nmap.org

³⁷ "Tenable Nessus", tenable.com

³⁸ "Nikto2", cirt.net

³⁹ "Security Recommendations for TLS", cyber.gouv.fr

⁴⁰ "ANSSI's Publications", cyber.gouv.fr

⁴¹ "Recommendations to secure administration of IT systems", cyber.gouv.fr

⁴² "Recommandations pour la mise en place de cloisonnement système", cyber.gouv.fr

FACTSHEET 10 – SECURING WEBSITES

Ensure that minimum good practices are applied to websites.

Every website must guarantee its identity to the terminals connecting to it and the confidentiality of the information transmitted.

Basic precautions

- **Secure data exchange flows through the use of TLS:**
 - **obtain certificates** at the appropriate levels (domain, organisation or extended) from a certification authority and manage them appropriately;
 - implement the **TLS** (replacing SSL⁴³) protocol on all websites, using only the latest versions and verifying its correct implementation;
 - **make the use of TLS mandatory** for all authentication pages or pages on which personal data are displayed or transmitted.
- **Limit communication ports** to those strictly necessary for the proper functioning of installed applications. If access to a web server is only via HTTPS, you should allow only incoming IP network traffic for that machine on port 443 and block all the other ports.
- **Restrict access to administrative tools and interfaces to authorised personnel only.** In particular, restrict the use of administrator accounts to internal IT teams, and only for administrative actions that require them.
- Implement the “HttpOnly” and “secure” options for all cookies used.
- **If cookies that are not necessary for the service are used, collect the user’s consent** after informing the user and before the cookie is stored.
- **Limit the number of components used**, monitor them regularly and update them.
- **Limit the information returned when creating a user account or when resetting a password**, in order not to inform an attacker about the existence – or not – of an account associated with an identifier (e.g. e-mail address).
- **Adopt best practices for IT development** (see [factsheet 11 – Managing IT developments](#)). In particular, **guard against the most common attacks on websites referenced in the OWASP Top 10**⁴⁴ (e.g.: SQL injections⁴⁵, XSS injections⁴⁶, URL manipulations⁴⁷).

What should be avoided

- Transmitting personal data in a URL (e.g.: credentials, passwords).
- Using unsecured services (e.g.: unencrypted authentication, unencrypted flow).
- Using servers hosting websites as workstations (e.g.: browsing websites, e-mail access).
- Placing databases on a server directly accessible from the Internet.
- Using generic user accounts (i.e. shared between several users).

⁴³ The TLS protocol is sometimes wrongly called SSL or SSL/TLS. The SSL protocol, the predecessor of TLS, is now obsolete and to be banned.

⁴⁴ The Open web application security project (OWASP) regularly publishes a list of the ten most critical risks for web applications (see “OWASP Top Ten”, [owasp.org](#)).

⁴⁵ “SQL Injection”, [owasp.org](#)

⁴⁶ “Cross Site Scripting (XSS)”, [owasp.org](#)

⁴⁷ “Path Traversal”, [owasp.org](#)

TO GO FURTHER

- Regarding the implementation of cookies, it is advisable to consult the dedicated dossier on the CNIL website⁴⁸.
- Generally speaking, comply with the L1 and L2 levels of the recommendations produced by OWASP. If for⁴⁹ software running on servers, it is advisable to use **vulnerability detection tools** (vulnerability scan software such as OWASP ZAP⁵⁰, nmap⁵¹ or nikto⁵²) for the most critical processing, in order to detect possible security flaws. Systems for detecting and preventing attacks on critical systems or servers can also be used. These tests must be carried out on a regular basis and before any new software version is put into production.
- **The ANSSI has published specific recommendations on its website⁵³** for implementing TLS⁵⁴ or securing a website⁵⁵.

⁴⁸ "Site web, cookies et autres traceurs", cnil.fr

⁴⁹ "OWASP MAS Checklist", mas.owasp.org

⁵⁰ "Zed Attack Proxy (ZAP)", zaproxy.org

⁵¹ "Nmap", nmap.org

⁵² "Nikto2", cirt.net

⁵³ "ANSSI's Publications", cyber.gouv.fr

⁵⁴ "Security Recommendations for TLS", cyber.gouv.fr

⁵⁵ "Sécuriser un site web", cyber.gouv.fr

FACTSHEET 11 – MANAGING IT DEVELOPMENTS

Integrate the security and protection of personal data as early as possible into projects.

The protection of personal data must be integrated into the IT development cycle right from the design phase and for default configurations in order to provide data subjects with better control over their data and to limit errors, losses, unauthorised changes, or misuse of their data in applications.

Basic precautions

- **Integrate data protection, including its data security requirements, from the design** of the application or service. These requirements can result in a variety of architecture choices (decentralised or centralised), of functionalities (e.g.: anonymisation done shortly after collection, data minimisation), of technologies (e.g.: communication encryption), etc.
- **Use community-recognised and secure** components (e.g.: libraries) or tools.
- Implement measures against common attacks targeting databases (e.g.: SQL code injections, scripts).
- **For any development aimed at the general public, carefully consider the parameters affecting privacy and its compliance**, in particular the default settings.
- **Avoid the use of free text boxes or comments**, which are sources of unnecessary or disproportionate additional personal data collection.
- **Carry out comprehensive tests** (e.g.: unit, integration, functional, security testing) before a product is made available or updated. During an update, make sure that the tests used are always appropriate.
- Carry out computer development and testing in a distinct computer environment from production (e.g. on different computers or virtual machines) and on fictitious or anonymised data.
- **Ensure that there are no secrets (authentication or encryption)** when submitting code to a version management tool (e.g.: Git or svn). **Change the secrets when going into production.**
- **Perform a non-regression test and/or a code review before any update goes to production**, in order to avoid the emergence of sources of personal data breach.

What should be avoided

- Using real personal data for the development and testing phases. Fictitious datasets should be used as much as possible.
- Developing an application and then think about the security or protection measures to be put in place regarding personal data.

TO GO FURTHER

- The CNIL has published a **GDPR guide**⁵⁶ **specifically aimed at development teams** to help them bring their IT developments into line with the regulations regarding the protection of personal data.
- **Put in place a defence in depth of systems**, i.e. a combination of several security measures and controls (e.g. control data entered in an online form but also protect database queries). In particular, the measures in place on the “frontend” part of an application can be circumvented and should be reinforced by measures on the “backend” part.
- Development must impose **data entry and recording formats that minimise the data collected**. For example, if only a person’s year of birth is to be collected, the field of the corresponding form should not allow the entry of the month and day of birth. This can mean, in particular, the implementation of a drop-down menu limiting the choices for a form field.
- An article dedicated to free text or comment zones is available on the CNIL website.⁵⁷
- Coding conventions or rules and documentation are essential to maintain the application or service over time without introducing new vulnerabilities, and to effectively correct malfunctions.
- Data formats must be compatible with the implementation of the chosen retention period. For example, if a digital document is to be kept for 20 years, it may be relevant to favour open formats that are more likely to be maintained over the long term.
- The **creation and management of user profiles** with data access rights varying according to the categories of users must be integrated right from the design phase.
- Tests carried out on fictitious or anonymised data are sometimes not sufficient to ensure that a new service or feature works properly. It is then possible to test in a pre-production environment with real data. The pre-production environment must be configured and secured at the same level as the production environment itself and the new service or its update must have already undergone all the tests (unit, integration and functional) in the development and testing environments.
- Depending on the nature of the application, it may be necessary to ensure its integrity by using executable code signatures in order to ensure that it has not undergone any alteration.

⁵⁶ “Guide RGPD de l’équipe de développement”, lincnil.github.io

⁵⁷ “Zones bloc note et commentaires : les bons réflexes pour ne pas déraper”, cnil.fr

FACTSHEET 12 – PROTECTING THE PREMISES

Strengthen the security of premises hosting computer servers and network hardware.

Access to premises must be controlled to prevent or slow down unauthorised direct access, whether to paper files or computer equipment, including servers. Premises must also be protected against other types of threats (e.g. fire, flood).

Basic precautions

- Restrict access to premises by means of locked doors.
- Install **intrusion alarms** and check their proper operation periodically.
- **Set up smoke detectors and firefighting equipment**, and inspect them annually.
- Protect keys allowing access to premises as well as alarm codes.
- **Distinguish building areas according to risk** (e.g.: provide a dedicated access control for the computer room).
- Keep an up-to-date list of persons or categories of persons authorised to enter each area and periodically review this list.
- **Establish rules and means of controlling visitor access**, at least by **having visitors accompanied⁵⁸ outside public reception areas** by a person belonging to the organisation.
- Protect network access (e.g.: office sockets, patch bays) and allow only authorised equipment to connect to them.
- Physically protect computer equipment with specific measures (e.g.: dedicated firefighting system, elevation against possible flooding, power supply redundancy, air conditioning system redundancy).

What should be avoided

- Under designing or neglecting the maintenance of computer room environments (e.g.: air conditioning, uninterrupted power supply). A breakdown in these installations often results in the shutdown of machines or access to the rooms being opened (to promote air circulation) which effectively neutralises the elements contributing to the physical safety of the premises.
- Leaving visible (e.g.: screens of the secretariat easily readable by visitors, meeting rooms with screens visible from the outside) or accessible (e.g.: critical printed documents placed in public view in reception areas) data that should remain confidential.

⁵⁸ From their entrance, during their visit and until they leave the premises.

TO GO FURTHER

- Keep a record of access to rooms or offices likely to contain material processing personal data that could have a serious negative impact on data subjects in the event of an incident. **Inform users** of the implementation of such a system, after information and consultation with staff representative bodies.
- Ensure that only duly authorised personnel are admitted to restricted access areas. For example:
 - inside regulated areas, require all persons to wear a visible means of identification (e.g.: badge);
 - visitors (e.g.: technical support staff) must only have limited access. The date and time of their arrival and departure must be recorded;
 - regularly review and update access permissions to secure areas and delete them if necessary.

MY CONTROL OVER DATA

FACTSHEET 13 – SECURING EXCHANGES WITH THE OUTSIDE WORLD

Strengthen the security of any transmission of personal data.

Without additional measures, consumer data transmission channels (e.g. email, instant messaging, file storage platforms) **are rarely a secure means of communication** for transmitting personal data. A simple careless mistake can lead unauthorised persons to gain access of personal data, thereby infringing the right to privacy of the data subjects. In addition, entities with access to the servers through which the information transits may have access to their content or metadata.

Basic precautions

- **Encrypt data before it is stored on a physical medium to be transmitted to a third party** (e.g. USB drive, portable hard drive, optical disk).
- **When sending via a network:**
 - **encrypt the sensitive parts** to be transmitted. In this regard, you should refer to the recommendations in [factsheet 21 – Encryption, hash, signature](#);
 - use a protocol that ensures confidentiality and authentication of the destination server for file transfers (e.g. **SFTP** or **HTTPS**), using the **most recent versions of the protocols**;
 - **ensure confidentiality of secrets** (e.g.: encryption key, password) by transmitting them via a separate channel from protected data (e.g.: sending the encrypted file by e-mail and communicating the password by phone or SMS).
- Open a file from outside only if the sender is known and after only after an **antivirus scan** has been carried out.
- When using a **fax** machine, put in place the following measures:
 - install the fax machine in a physically controlled room and accessible only to authorised staff;
 - display the identity of the fax recipient when sending messages;
 - double the sending by fax with a sending of the original documents to the recipient;
 - pre-register the numbers of potential recipients in the fax address book (if the function exists).

What should be avoided

- Transmitting files containing unencrypted personal data via messaging or other consumer platforms.
- Not planning for the deletion (preferably automatically) of files transmitted using a file transfer platform.

TO GO FURTHER

- Use public key algorithms, when different actors have put a **public key management infrastructure** in place to ensure the confidentiality and integrity of communications, as well as the authentication of the issuer.
- Have **the data electronically signed** by the issuer before it is sent in order to ensure that she or he is the originator of the transmission ([see factsheet 21 – Encryption, hash, signature](#)).
- Use of a **temporary file repository server** may also be appropriate. In this case, ensure to:
 - set up a limited time for making files available;
 - restrict access to files to only duly authorised recipients;
 - encrypt files before uploading them to the service if the solution used does not provide for this possibility in an integrated way.
- Some communication tools and solutions also protect metadata related to the items being exchanged and can be used when these are particularly sensitive.
- For the most sensitive systems, confine files from outside to isolated areas from the rest of the system to prevent the spread of malware.

FACTSHEET 14 – MANAGING DATA PROCESSORS

Manage data security with processors.

Data processing carried out by a processor on⁵⁹ behalf of the controller must be subject to sufficient safeguards, in particular in terms of security. The data controller must be aware of the details of the security measures implemented by its processors in order to be able to demonstrate its compliance⁶⁰.

Basic precautions

- **Use only processors with sufficient guarantees** (particularly in terms of specialised knowledge, reliability and resources).
- **Provide for a contract with the processors**⁶¹, which defines in particular the subject matter, duration, purpose of the processing as well as the obligations of the parties, in particular in terms of security. Ensure that it contains, in particular, provisions setting out:
 - the division of responsibilities and obligations relating to the confidentiality of the personal data entrusted;
 - minimal user authentication requirements;
 - the conditions for the return and destruction of data at the end of the contract;
 - the rules for managing and notifying incidents. These should include informing the controller in the event of a discovery of a security breach or incident, and this should be done as soon as possible in the event of a personal data breach⁶²;
 - assistance to be provided to the processor to ensure compliance with security obligations⁶³;
 - the regular review of security measures and, where appropriate, the conditions for their revision.
- **Provide the means to verify the effectiveness of the data protection guarantees offered by the processor** (e.g.: security audits, site visits). Such guarantees include, but are not limited to:
 - the encryption of data according to their sensitivity or, failing that, the existence of procedures ensuring that the service company does not have access to the data entrusted to it if this is not necessary for the performance of its contract;
 - encryption of data transmissions (e.g.: HTTPS connection, VPN implementation);
 - guarantees in terms of network protection, traceability, authorisation management, authentication, administrator practices, audits, etc.

What should be avoided

- Starting processing data without having signed a contract with the processor that includes the requirements laid down in Article 28 of the GDPR.
- Using cloud services without guarantee as to the actual geographical location of the data and without ensuring legal conditions and any possible formalities for data transfers outside the European Union.

⁵⁹ Understood within the meaning of the GDPR.

⁶⁰ Articles 5.2 and 24.1 of the GDPR.

⁶¹ The European Commission has published standard contractual clauses on which this contract may be based (see “Clauses contractuelles types entre responsable de traitement et sous-traitant”, cnil.fr).

⁶² A security incident is characterised as a “personal data breach” when it relates to personal data.

⁶³ Refer to Article 32 of the GDPR and § 41 of Guidelines 07/2020 adopted by the European Data Protection Board (EDPB)

POUR ALLER PLUS LOIN

- The CNIL has published a guide for processors⁶⁴.
- Consult and implement the provisions of Article 28 GDPR.
- Pay particular attention to the choice of a cloud service provider ([see factsheet 22 – Cloud computing](#)).
- The entire sub processing chain (processors of processors) should be considered and not only direct processors.
- When choosing a processor, obtaining a certification is a first index to assess its reliability. For example, the international standard ISO/IEC 27001⁶⁵ requires organisational and technical measures for the establishment of an Information Security Management System (ISMS), while ISO/IEC 27701 covers Privacy Management Systems (PIMS).
- Regarding health data, a hosting provider must have a health data hosting (HDS) certification⁶⁶. The Digital Health Agency (ANS) publishes a list of certified hosting providers. It is worth noting that a certification process has gradually replaced the HDS authorisations since 2018 and that some hosting providers⁶⁷ still have a⁶⁸ valid authorisation.
- Where appropriate, require the service provider to communicate its certifications and verify their scope.

⁶⁴ "Règlement européen sur la protection des données : un guide pour accompagner les sous-traitants", cnil.fr

⁶⁵ "L'ISO 27701, une norme internationale pour la protection des données personnelles", cnil.fr

⁶⁶ "Health Data Hosting (HDS)", esante.gouv.fr

⁶⁷ "Liste des hébergeurs certifiés", esante.gouv.fr

⁶⁸ "Liste des hébergeurs agréés", esante.gouv.fr

FACTSHEET 15 – SUPERVISING THE MAINTENANCE AND END-OF-LIFE OF HARDWARE AND SOFTWARE

Ensure data security at every stage of the hardware and software lifecycle.

Support operations must be supervised to control access to data by service providers. The data must first be erased from equipment destined for disposal.

Basic precautions

- **Record maintenance interventions in a log book.**
- **Open the access required** for remote maintenance **at the service provider's request**, for a pre-defined period of time appropriate for the intervention. These accesses must be closed again at the end of this period.
- Include security clauses in maintenance contracts with service providers to control their access to information systems (see sample clause opposite).
- **Ensure that third-party interventions are supervised by an organisation manager.**
- **Do not leave outside contractors alone**, especially in sensitive rooms (e.g. server rooms).
- **Securely delete the data from equipment before its disposal, its sending for repair to a third party** or at the end of a rental contract.

What should be avoided

- Installing remote maintenance applications with known vulnerabilities (e.g.: applications that do not encrypt communications).
- Reusing, reselling or discarding media that have contain personal data without the data having been securely deleted.
- Allowing full or permanent access to systems for remote maintenance.

TO GO FURTHER

- Write and implement a secure data deletion procedure.
- Use software dedicated to deleting data without physical destruction that has been qualified or certified. ANSSI grants first-level certifications⁶⁹ to such software.
- Implement real-time or a posteriori (e.g.: recording) monitoring tools (e.g. "4-eye" sessions) for remote maintenance interventions by third parties⁷⁰.
- ANSSI dedicates a chapter of its guide⁷¹ on secure administration to third-party maintenance.

⁶⁹ "Certified products", cyber.gouv.fr

⁷⁰ Like logging systems, such systems must be set up in accordance with the applicable legal provisions and with information of the data subjects.

⁷¹ "Recommendations to secure administration of IT systems", cyber.gouv.fr

Example of a clause that can be used in case of maintenance by a third party:

Each maintenance operation must be the subject of a description specifying the dates, the nature of the operations and the names of the involved participants, transmitted to X.

In case of remote maintenance allowing remote access to X's files, Y will only be able to intervene after X has authorised access. Access must be closed at the end of each Y intervention.

[Alternative formulation according to the nature of maintenance:

In case of remote maintenance allowing remote access to X's files, Y will only be able to intervene after X has been informed, allowing X to identify and monitor access to its information system.

]

Records will be established under the respective responsibilities of X and Y, indicating the date and detailed nature of the remote maintenance interventions and the names of their authors.

Note: such a maintenance clause must necessarily be coupled with a confidentiality clause for processors.

PREPARING FOR AN INCIDENT

FACTSHEET 16 – LOGGING OPERATIONS

Log operations for the detection of anomalies, malfunctions or incidents and have the information useful for their treatment or in the event of litigation.

In order to be able to **identify fraudulent access** or **misuse** of personal data, or to determine the origin of an incident, it is necessary to log certain actions carried out on IT systems. The logs then collected are also useful evidence for the demonstration of compliance⁷².

Basic precautions

- **Provide a logging system** (i.e. recording system in log files) of users' business activities (application logs), technical interventions (including by administrators), anomalies and security-related events (technical or system logs).
- **Keep these logs for a rolling period of between six months and one year** (except, for example, in the event of a legal obligation relating to this retention period, the need for litigation management, internal control or an identified need for post-incident analysis).
- **Perform, for application logs, a record of the creation, consultation, sharing, modification and deletion** of the data by retaining the author's identifier, the date, time and nature of the operation as well as the reference of the data concerned (to avoid duplication).
- **Inform users**, e.g. when authenticating or accessing the system, of setting up the logging system, after informing and consulting the representative bodies of the staff.
- **Protect the logging equipment and the logged information** against unauthorised operations (e.g. by making them inaccessible to the individuals whose activity is logged), misuse by authorised accounts (e.g.: by setting up a use charter or specific alerts) and the crushing of logs generated by the concerned applications.
- Ensure the proper functioning of the logging system **by integrating the equipment into a monitoring tool and regularly checking the presence of exploitable logs**.
- **Ensure that processors are contractually obliged** to implement logging in accordance with these recommendations and to notify as soon as possible of any anomaly or security incident to the controller.
- **Actively analyse, in real time or in the short term, the logs collected to be able to detect the occurrence of an incident** ([see factsheet 9 – Managing incidents and violations](#)).

What should be avoided

- Duplicating and storing excessively the personal data concerned by the processing within the logs (e.g.: saving passwords or their hash when authenticating users).
- Using information from logging systems for purposes other than ensuring the proper use of the computer system (e.g. using logs to count hours worked is a misuse of purpose, punishable by law).
- Keeping logs without time limit.

⁷² Articles 5.2 et 24.1 du RGPD.

TO GO FURTHER

- See the CNIL recommendation on logging⁷³.
- **Involve the user in the monitoring of transactions carried** out on his account and his data (e.g.: provide a summary of the last three connections). Focus on automatic monitoring of logs, coupled with an appropriate configuration of alerts.
- **Set up a collection enclave** centralising event logs throughout the information system in order to prevent any alteration thereof.
- ANSSI has published recommendations on the setting up of a logging system⁷⁴ and more specifically recommendations in the Active Directory environment⁷⁵.

⁷³ "La CNIL publie une recommandation relative aux mesures de journalisation", [cnil.fr](https://www.cnil.fr/fr/recommandation-relationnelle)

⁷⁴ "Recommandations de sécurité pour l'architecture d'un système de journalisation", cyber.gouv.fr

⁷⁵ "Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory", cyber.gouv.fr

FACTSHEET 17 – SAVING

Perform regular backups to limit the impact of an unwanted data loss or alteration.

Backup copies must be made and tested regularly to be available when needed.

Basic precautions

- **Make frequent data backups**, whether in paper or electronic form. It may be appropriate to provide incremental daily⁷⁶ backups and full backups at regular intervals.
- Store at least one backup on a site geographically separate from the operating site.
- **Isolate at least one offline backup**, disconnected from the company's network.
- **Protect stored data at the same level of security as those stored on operating servers** (e.g. by encrypting the backups, by providing storage in a secure place, by contractually framing a service of externalisation of backups).
- Encrypt the transmission channel, if it is not internal to the organisation, when backups are transmitted through the network.
- Regularly test the integrity of backups and the ability to restore them.

What should be avoided

- Ensuring a lower level of security on the backup system (e.g.: do not save the system itself) only on other information systems.
- Keeping backups on the same systems as the backed-up data without isolating them. A threat (e.g.: ransomware) could then tackle both data and their backups.
- Keeping backups in the same place as the machines hosting the data. A major disaster occurring there would result in a definitive loss of data.
- Never checking if backups are available and realising that this is not the case on the day they are needed.

TO GO FURTHER

- Protect at least one backup (e.g.: the one that is geographically distinct from the operating site) in fireproof and waterproof safes.
- If data and system availability requirements are high, it is advisable to implement data replication to a secondary site.
- It is advisable to apply the rule called “3 – 2 – 1”, state of the art in terms of backup, which consists of having 3 copies of the data, storing on 2 different media, including 1 offline.
- ANSSI has published recommendations⁷⁷ on the safeguarding of information systems.

⁷⁶ An incremental backup consists of saving only changes made compared to a previous backup.

⁷⁷ “Sauvegarde des systèmes d'information”, cyber.gouv.fr

FACTSHEET 18 – PREDICTING CONTINUITY AND RESUMPTION OF ACTIVITY

Predict degraded operation of information systems and be able to restart them without impacting data security.

To limit the downtime of the system, it is necessary to anticipate the most common incidents. Ensuring business continuity consists of planning ways to continue to operate, in general in a degraded manner, despite malfunctions. The resumption of activity, on the other hand, encompasses all the actions necessary to relaunch an established system.

Basic precautions

- **Write a business continuity plan (BCP) and a disaster recovery plan (DRP)**, even summary, for IT activity, including the list of stakeholders. The level of data protection should not be reduced by the intended operating modes.
- **Ensure that users, service providers and subcontractors know who to alert in the event of an incident.**
- **Regularly test the restoration of backups and the application of the business continuity plan or disaster recovery plan.**
- About materials:
 - use an inverter to protect equipment used for essential treatments;
 - provide for material redundancy of storage equipment (e.g.: using RAID technology⁷⁸).

What should be avoided

- Considering yourself safe.
- Reducing the level of data security when implementing a degraded procedure, without taking into account the new risks generated to maintain the activity.
- Not anticipating a return to normal.
- Not testing upstream business continuity or recovery measures.

TO GO FURTHER

- The General Secretariat for Defence and National Security (SGDSN) has published⁷⁹ a guide on the establishment of a business continuity or business resumption plan.
- Define a crisis management organisation.
- Carry out exercises with all stakeholders to verify the effectiveness and assimilation of the procedures put in place.
- Targeted tests on certain components or parts of the system may be preferred to limit the impact on production. However, the continuity and resumption of the most critical elements must be tested from time to time. A test of the complete shutdown of the information system should also be considered.

⁷⁸ RAID (redundant array of independent disk) refers to data distribution techniques on multiple storage media (e.g.: hard drives) to prevent data loss following the failure of one of the medias.

⁷⁹ "Bienvenue sur le guide de la continuité d'activité", guide-continuite-activite.sgdsn.gouv.fr.

FACTSHEET 19 – MANAGING INCIDENTS AND VIOLATIONS

Provide procedures for managing incidents and responding to data breaches (infringement of confidentiality, integrity or availability).

It is necessary to be prepared for the possibility of an incident to intervene in a timely and appropriate manner, incorporating the objective of limiting the effects for the persons whose data are concerned. The data controller may be required to notify the CNIL or inform the data subjects of the incident depending on the risk to them.

Basic precautions

- **Regularly analyse the logs collected** ([see factsheet 16 – Logging operations](#)).
- Ensure that **the managers of the logging management system** (whether internal or external) **notify the controller, as soon as possible, in the event of an anomaly or security incident**.
- Disseminate to all users, both internal and external, **the conduct to be followed and the list of persons to be contacted in the event of a security incident or an unusual event** affecting the organisation's information and communication systems. **Make users aware** of the importance of reporting suspicious events.
- Establish procedures detailing the systems for generating and raising alerts from different sources (e.g.: automatic, by users) their processing and the actions to be taken in the event of a proven incident (e.g.: persons to contact, actions to limit the incident according to its nature). Include data breach management in the incident management process. **Define criteria for classifying an incident as data breaches**.
- **Assess the risk to individuals caused by the violation**, taking into account the seriousness and likelihood of the consequences that the violation may have on their rights and freedoms.
- **Keep an internal record of all personal data breaches**.
- **Notify⁸⁰ the CNIL, within 72 hours (as provided for in the GDPR), of violations posing a risk to the rights and freedoms of individuals** and, in the event of a high risk and unless otherwise provided by the GDPR⁸¹, **inform the data subjects** so that they can limit the consequences⁸².

What should be avoided

- Waiting for data subjects or third parties to detect and report an incident.
- Omitting the analysis of the risks that a personal data breach could have for the rights and freedoms of individuals.
- Waiting for accurate information to notify the CNIL when it is clearly established that a breach has occurred. Data notifications can be transmitted in two stages: an initial, within 72 hours, then an additional if necessary.

⁸⁰ The notification procedure is detailed on the CNIL website (see "Notifier une violation de données personnelles", [cnil.fr](#)).

⁸¹ Articles 33 and 34 of the GDPR.

⁸² The obligation to notify personal data breaches does not relieve the person responsible of his/her potential other incident reporting obligations (see "Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ?", [cnil.fr](#)).

TO GO FURTHER

- Focus on **automatic monitoring of logs**, coupled with an appropriate configuration of alerts.
- Establish mandatory training for all staff on identifying and reporting violations as well as on what to do in this case.
- The EDPS⁸³ published guidelines⁸⁴ detailing 18 examples of data breaches, based on practical cases encountered by European data protection authorities.
- The Working Party (referred to as “Article 29”) which preceded the EDPS on data protection also published guidelines⁸⁵ on the notification of personal data breaches to accompany bodies in the implementation of their obligations.
- In the event of an incident or to prepare for it, consult the digital security assistance and prevention website⁸⁶.

⁸³ European Data Protection Board.

⁸⁴ “Guidelines 01/2021 on Examples regarding Personal Data Breach Notification”, edpb.europa.eu

⁸⁵ “Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)”, ec.europa.eu

⁸⁶ “Assistance et prévention du risque numérique au service des publics”, cybermalveillance.gouv.fr

FOCUS

FACTSHEET 20 – RISK ANALYSIS

Identify risks and assess their likelihood and severity in order to implement the appropriate security measures.

Besides complying with the basic precautions presented in this guide, it is relevant, if not mandatory according to the criticality of the processing, to carry out data protection risk analyses. These analyses provide a basis for deciding on additional security measures, adapted to the context, to limit the impact on the data subjects involved in the data processing.

Basic precautions

- Identify the processing of personal data for which **a data protection impact assessment (DPIA)⁸⁷ must be carried out in accordance with the GDPR⁸⁸**. A PIA includes not only a part dedicated to risks analysis, the topic of this factsheet, but also a part dedicated to the legal aspects of the data processing.
- Carry out a risk analysis⁸⁹, even a minimal one, based on the following three steps:

1. Identify 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 systems, business software);
- the cloud computing resources used (e.g.: SaaS, PaaS, IaaS);
- the logical or physical communication channels (e.g.: wired connections, Wi-Fi, Internet, verbal exchanges, couriers);
- the paper documents (e.g.: printed documents, photocopies);
- the physical premises and facilities where the above-mentioned elements are located (e.g.: IT rooms, offices).

This step deserves to be carried out independently of any risk analysis ([see factsheet 1 – Managing data security](#)).

2. Assess the risks generated by each processing operation:

- a. Identify potential effects** on the rights and freedoms of data subjects, for the three following feared events:
- **illegitimate access to data** (e.g.: identity theft following the disclosure of pay slips for all employees of a company);
 - **unwanted data modification** (e.g.: wrongful accusation of a fault or offence following the modification of access logs);
 - **temporary or permanent loss of data** (e.g.: failure to detect a drug interaction due to the impossibility of accessing the patient's electronic record).

⁸⁷ "Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)", cnil.fr

⁸⁸ Article 35 of the GDPR.

⁸⁹ The vocabulary used in the following description is taken from the AIPD guides published by the CNIL (see "Privacy Impact Assessment (PIA)", cnil.fr).

b. Identify the sources of risk (who or what could be at the origin of each feared event?), taking into account internal and external human sources (e.g. it administrator, user, external attacker, competitor) as well as internal and external non-human sources (e.g. water, epidemic, hazardous materials, non-targeted computer virus).

c. Identify the possible threats (what could allow each feared event to occur?). These threats occur on previously identified media (hardware, software, communication channels, paper documents, etc.), which may 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.: observation of a screen on a train, geolocation of equipment);
- damaged (e.g.: vandalism, degradation due to natural wear);
- overloaded (e.g.: full storage unit, denial of service attack).

d. Identify existing or planned measures to reduce each risk (e.g.: access control, backups, traceability, security of the premises, encryption, anonymisation).

e. Evaluate the severity (impact or potential harm to the data subjects) and the likelihood (probability of occurrence) of the risks with regard to the previous elements (an example of scale that can be used for the evaluation: negligible, moderate, large, maximum).

Feared event	Effects on individuals	Main sources of risk	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access of data						
Unwanted modification of data						
Loss of data						

The following table can be used to formalise this reflection:

3. Implement and check the planned measures. If the existing and planned measures are considered appropriate, it must be ensured that they are implemented and monitored ([see factsheet 1 – Managing data security](#)). Otherwise, additional measures must be identified and implemented to reduce the severity and/or likelihood of the associated risks.

- **Regularly review the risk analysis** and, in particular, in the event of a change in the system or the treatment context.

What should be avoided

- Forgetting the impact for data subjects and only considering the impact for the organisation.
- Omitting part of the data processing (e.g.: collection, partners, end-of-life data) to conduct the analysis.
- Adjust scales of likelihood and severity during the risk analysis, rather than defining them upstream based on the overall context of the organisation.

TO GO FURTHER

- The GDPR introduces **Data Protection Impact Assessments** (DPIA) and specifies that they shall contain at least “a [...] description of the [...] operations and the purposes of the processing [...], an assessment of necessity and proportionality [...], an assessment of the risks [...] and the measures envisaged to address the risks [...] and to demonstrate compliance with the Regulation” (Article 35.7).
- The CNIL has published guides⁹⁰ to conduct a DPIA. The CNIL has also published software to facilitate the conduct and formalisation of DPIA⁹¹.
- The CNIL has also published lists of processing for which a DPIA is required⁹² or not⁹³.
- **Security audits are an essential means of assessing the level of security of the systems on which the processing of personal data is based.** Carried out periodically, they allow to take changes in processing and threats into account. Each audit must produce an action plan, the implementation of which should be monitored at the highest level of the organisation.
- **The assessment of information security risk⁹⁴ may be conducted at the same time as the assessment of privacy risk.** These approaches are compatible.
- The risk assessment provides a basis for determining the security measures to be put in place. **Allocate a budget** for their implementation is required.

⁹⁰ “Privacy Impact Assessment (PIA)”, cnil.fr

⁹¹ “The open source PIA software helps to carry out data protection impact assessment”, cnil.fr

⁹² “Analyse d’impact relative à la protection des données : publication d’une liste des traitements pour lesquels une analyse est requise”, cnil.fr

⁹³ “Analyse d’impact relative à la protection des données : publication d’une liste des traitements pour lesquels une analyse n’est pas requise”, cnil.fr

⁹⁴ For example, using the EBIOS RM method (see “EBIOS Risk Manager – The method”, cyber.gouv.fr), the risk management method published by the ANSSI, an agency attached to the General Secretariat for Defence and National Security (“Secrétariat général de la défense et de la sécurité nationale” or SGDSN). EBIOS is a registered trademark of SGDSN.

FACTSHEET 21 – ENCRYPTION, HASH, SIGNATURE

Ensure the integrity, confidentiality and authenticity of information.

Hash functions ensure **data integrity**. **Digital signatures**, in addition to ensuring integrity, make it possible to verify the signatory's identity authenticity and to ensure the non-repudiation. Finally, **encryption**⁹⁵ ensures **the confidentiality** of a message.

Basic precautions

- **Use a recognised and safe algorithm**, for example, the following algorithms:
 - SHA-2⁹⁶ or SHA-3⁹⁷ as hash function families;
 - bcrypt, scrypt, Argon2 or PBKDF2 to store passwords;
 - AES⁹⁸ with an appropriate construction mode (CCM, GCM, or EAX) or ChaCha20⁹⁹ (with Poly1305) for symmetric encryption;
 - RSA-OAEP¹⁰⁰, ECIES-KEM¹⁰¹ or DLIES-KEM101¹⁰¹ for asymmetric encryption;
 - RSA-SSA-PSS100¹⁰⁰ or ECDSA¹⁰² for signatures.
- **Use sufficiently long keys**:
 - for AES, 128, 192 or 256 bit keys are considered sufficient;
 - for RSA-based algorithms, it is recommended to use secret modulus and exponents of at least 2048 bits or 3072 bits, with public exponents, for encryption greater than 65536 bits.
- **Apply relevant recommendations for use**, specific to the chosen algorithm. Implementation errors have a significant impact on the security of the cryptographic mechanism.
- **Protect private keys**, at least through the implementation of limited access rights and a secure password.
- **Write a procedure indicating how keys and certificates will be managed** considering cases of forgotten passwords for unlocking them.

What should be avoided

- Using outdated algorithms, such as DES and 3DES encryption or MD5 and SHA-1 hash functions.
- Confusing hash functions with encryption functions and considering that a hash function alone is enough to guarantee data confidentiality. Although hash functions are “one-way” functions, i.e. functions that are difficult to reverse, data can be retrieved from its fingerprint. Indeed, since these functions are fast at execution, it is often possible to automatically test all the possibilities and thus recognise the footprint.
- Hashing passwords without using any salt¹⁰³.

⁹⁵ Sometimes improperly called encryption.

⁹⁶ As defined in the NIST FIPS 180-4 standard.

⁹⁷ As defined in NIST FIPS 202.

⁹⁸ As defined in NIST FIPS 197.

⁹⁹ As defined in RFC 8439.

¹⁰⁰ As defined in RSA PKCS#1 v2.2.

¹⁰¹ As defined in ISO/IEC 18033-2.

¹⁰² As defined in NIST FIPS 186-5.

¹⁰³ We call “salt” a different hazard used for each password stored.

TO GO FURTHER

- See the dedicated page on the CNIL website¹⁰⁴.
- ANSSI has published **guides**¹⁰⁵ to assist **developers and administrators in their choice of cryptographic algorithms, sizing and implementation**.
- When receiving an electronic certificate, **verify that the certificate** contains an indication of use in accordance with what is expected, **that it is valid and not revoked, and that it has a correct chain of trust** at all levels.
- **Use cryptographic software or libraries that have been verified by third parties with proven expertise.**
- Different encryption solutions can be used, such as:
 - solutions certified or qualified by ANSSI¹⁰⁶ ;
 - VeraCrypt software, enabling the implementation of¹⁰⁷ encrypted containers;
 - the GNU Privacy Guard software, enabling the implementation of asymmetric cryptography (signature and encryption)¹⁰⁸.
- For administrative authorities, the Annexes to the General Security Repository (GSR)¹⁰⁹ shall apply, in particular Annexes B1 and B2 regarding cryptographic mechanisms and key management respectively.

¹⁰⁴ "Comprendre les grands principes de la cryptologie et du chiffrement", cnil.fr

¹⁰⁵ "Mécanismes cryptographiques", cyber.gouv.fr

¹⁰⁶ "Security VISA", cyber.gouv.fr

¹⁰⁷ A container is a file that may contain several other files.

¹⁰⁸ "The Gnu Privacy Guard", gnupg.org

¹⁰⁹ "Le référentiel général de sécurité version 2.0 : les documents", cyber.gouv.fr

FACTSHEET 22 – CLOUD COMPUTING

Secure data and processing in a cloud environment.

Cloud computing is perceived as a faster and more flexible way to deploy new services. However, implementing data processing shall always factor the specific risks relevant to cloud computing. The cloud service provider must provide sufficient guarantees to ensure that security measures were correctly implemented. Nonetheless, the client also has to be involved into securing their data and data processing in the cloud, not only to protect them from malicious third parties but also from the cloud service provider itself.

Basic precautions

- **Map data and processing in the cloud** and maintain this mapping up-to-date. Also map cloud services in use (including SaaS applications). Identify unused or unmonitored cloud resources, and if applicable, remove them.
- Assess the security needs for the implemented data processing then choose:
 - the appropriate **service deployment method** (public, private, hybrid, community, multi-cloud);
 - the cloud service provider after evaluating their guaranteed level of security (in particular for backups, redundancy, encryption, physical security, maintenance security) in accordance to recognised cloud security specifications.
- **Include cloud services into the risk analysis** ([see factsheet 20 – Risk analysis](#)), but also in the PCA/PRA ([see factsheet 18 – Predict continuity and resumption of activity](#)), while considering their specificities.
- **Make sure security requirements and liability allocation are covered by a contract between the supplier and the customer** ([see factsheet 14 – Managing data processors](#)).
- Ensure that **all parties involved** in the cloud service provisioning **actually maintain the level of security you agreed upon** (the provider itself and its potential subcontractors).
- **If relevant, configure the security tools provided by the provider** (e.g.: encryption, access and identity management, firewall, anti-DDoS tool) in accordance with the internal information systems security policy.
- Apply the **basic precautions** from this guide to cloud processing. In particular:
 - encrypt dormant data as well as transit data and use the appropriate cryptographic key management ([see factsheet 21 – Encryption, hash, signature](#)). Note that using the key management services offered by the service provider implies that the service provider also has the ability to access the data;
 - make sure **only authorized personnel are assigned with the relevant access** and permissions rights for resources access (data and applications) in the cloud and apply the principle of less privilege ([see factsheet 5 – Access management](#));
 - authenticate users for access to cloud services ([see factsheet 4 – Authenticating users](#)) and grant only the necessary authorisations ([see factsheet 5 – Access management](#));
 - manage and configure cloud resources permissions;
 - perform backups ([see factsheet 17 – Saving](#)) and check that your provider actually has several backup data centres that are geographically distant from each other.

What should be avoided

- Migrating all data and processing to the cloud, without identifying sensitive data that should not be processed in the cloud.
- Neglecting security aspects when selecting the cloud service provider.
- Assuming that the cloud security responsibility is solely lying with the provider.
- Having a lower security assurance level than locally performed processes.
- Forgetting to include telemetry data, diagnostic data and processing data collected by the provider in the risk analysis.
- Believing that server-side encryption ensures confidentiality with the provider.
- Not configuring or misconfiguring the security tools provided by the supplier¹¹⁰.
- Sharing authentication means (e.g.: hard-coded unencrypted identifiers or access keys in the source code files of applications or scripts executed in the cloud).
- Using cloud services without ensuring you got actual guarantees about the data physical and geographical location and without checking legal conditions and possible formalities for data transfers outside the European Union.
- Having a backup policy where the data is hosted in the same data centre as the backup.
- Signing a contract stating that the cloud provider can access data and systems for some purposes (including security or legal obligation), without the authorisation of the customer.

TO GO FURTHER

- **Conduct regular security audits of the supplier.**
- **Prioritise providers complying to GDPR codes of conduct**¹¹¹ and ensure that these codes of conduct contain specific security requirements and clarifications on cloud -specific regulatory obligations. See in particular the codes approved by the authorities after the opinion of the European Data Protection Board (EDPB): the CISPE code¹¹² or the EU Cloud code¹¹³.
- Consider the use of a supplier qualified under SecNumCloud¹¹⁴ by ANSSI for the processing of particularly sensitive data. Rule R9 of the “cloud at the center” doctrine¹¹⁵ requires the use of such a provider for some operators.
- Use a certified health data hosting provider¹¹⁶ (HDS) for the processing of health data in accordance with Article L1111-8 of the Public Health Code. The Digital Health Agency (ANS) publishes the list of certified hosts¹¹⁷. Note that certification has gradually replaced HDS approval since 2018 and that some hosts still have a¹¹⁸ valid approval.
- Consult the CNIL factsheet¹¹⁹ on encryption practices in the public cloud.
- Consult the CNIL factsheet¹²⁰ on tools for web application security in the cloud.

¹¹⁰ “Violation du trimestre : les défauts de configuration des espaces de stockage dans le cloud public”, cnil.fr

¹¹¹ “What you need to know about the code of conduct”, cnil.fr

¹¹² “La CNIL approuve le premier code de conduite européen dédié aux fournisseurs de services d’infrastructure cloud (IaaS)”, cnil.fr

¹¹³ “Eu Cloud COC”, eucoc.cloud

¹¹⁴ “L’ANSSI actualise le référentiel SecNumCloud”, cyber.gouv.fr

¹¹⁵ “Actualisation de la doctrine d’utilisation de l’informatique en nuage par l’État (« cloud au centre »)”, legifrance.gouv.fr

¹¹⁶ “Health Data Hosting (HDS)”, esante.gouv.fr

¹¹⁷ “Liste des hébergeurs certifiés”, esante.gouv.fr

¹¹⁸ “Liste des hébergeurs agréés”, esante.gouv.fr

¹¹⁹ “Les pratiques de chiffrement dans l’informatique en nuage (cloud) public”, cnil.fr

¹²⁰ “Les outils de sécurisation d’applications web dans l’informatique en nuage (cloud)”, cnil.fr

FACTSHEET 23 – MOBILE APPLICATIONS: DESIGN AND DEVELOPMENT

Apply basic security principles to mobile application development.

Mobile applications are one of the main means of accessing digital content and services and involve most of the time the processing of personal data. It is necessary for publishers to secure these processing and offer the best possible transparency to users.

Basic precautions

- **Minimise the processing of personal data** by ensuring that each type of data collected is indeed necessary for the operation of the application.
- Choose, when selecting, the permissions relevant to the operation of the application and involving the minimum additional collection, or even propose alternatives to the user not based on permissions (e.g.: geolocation can simplify a geographic search, but can be replaced by manual address entry).
- **Secure communications**, at least with servers, by encapsulating them in a TLS channel, respecting the ANSSI TLS guide¹²¹.
- **Store cryptographic secrets securely** by means of APIs allowing the use of cryptographic suites included in the phone, favouring hardware protections such as Android's Hardware Keystore¹²² or Apple's Secure Enclave¹²³.
- **Take into account the possibility of the operating system making automatic backups of any personal data.** Disable unwanted backups or encrypt data without including the encryption key in backups.
- **Use a means of authentication corresponding to the level of security sought** when authentication is required (e.g. if a person is to be authenticated with certainty, do not use biometric authentication if the device used allows the recording of biometric templates of several persons).

What should be avoided

- Contracting with a developer for the realisation of an application without properly defining with him the objectives and the technical measures expected in terms of data security and without specifying that these requirements are applicable to subsequent subcontractors ([see factsheet 14 – Managing data processors](#)).
- Integrate or allow its subcontractor to integrate in its application external code elements (or SDKs), including those proposed by the publishers of mobile operating systems, without ensuring that they themselves comply with state-of-the-art security precautions.

¹²¹ "Security Recommendations for TLS", cyber.gouv.fr

¹²² "Hardware-backed Keystore", source.android.com

¹²³ "Secure Enclave", support.apple.com

TO GO FURTHER

- In general, comply with levels L1 and L2 of the recommendations produced by the OWASP¹²⁴.
- **The mobile application security model should not be based on the integrity of the terminal (via a attestation made available by the operating system)**, except in certain justified cases. The service should be designed in such a way as to maintain the level of security even with terminals considered as corrupted. **Best practices in terms of APIs** ([see factsheet 25 – API: Application programming interfaces](#)) **should be applied to secure the servers used by the application and protect them against possible abuse attempts.**
- Prioritise the processing and storage of the user's data directly on his terminal.
- It is desirable that **the publisher of an application set up a process to validate all changes made to the processing implemented, in particular in terms of security**, in order to avoid changes (e.g.: maintenance operations, modification of external components) that could impact the overall security of the processing.
- It is important to implement processes that ensure the maintenance of the security of the application over time, including:
 - adopting a Continuous Integration and Deployment Methodology (CI/CD) to enable frequent application updates, especially in the case of security updates;
 - informing users of the availability of critical updates (e.g.: an information banner), or even by blocking certain server-level functionalities for insecure versions of the application;
 - maintaining vigilance regarding external elements embedded in applications, in particular in the face of the risk of malicious evolution in SDKs or libraries used, via supply chain security practices as described in ANSSI's analyses¹²⁵;
 - ensuring that the expected level of security can remain the same, for as long as possible, regardless of the version of the OS used. So that a user who would not want or could not access a recent device can benefit from a sufficient level of security.

¹²⁴ Open web application security project (see "OWASP MAS Checklist", mas.owasp.org).

¹²⁵ "Chaîne d'attaque sur les prestataires de service et les bureaux d'étude : un nouveau rapport d'analyse de la menace", cyber.gouv.fr

FACTSHEET 24 – ARTIFICIAL INTELLIGENCE: DESIGN AND LEARNING

Equip yourself with the necessary resources and tools to develop a robust, reliable and efficient AI system.

Whether training a new model or integrating an existing model into a software or an application ecosystem, the development of an artificial intelligence (AI) system requires the implementation of certain specific security measures. **The large volume of training data**, as well as the **complexity of these systems**, increases the attack surface and the risk of failure that can have serious consequences for the **reliability of the system**. This factsheet lists several **technical and organisational** recommendations to achieve a first level of safety.

Basic precautions

- Set up a **development team with multidisciplinary skills** (data analysis and engineering, user interface and user experience, quality control, IT infrastructure administration, business teams), ensure its training on good security practices and raise awareness of AI vulnerabilities.
- Implement a mandatory procedure for the continuous development and integration, based on **comprehensive and robust tests, access subject to authorisation and authentication adapted to the profiles** ([see factsheet 4 – Authenticating users](#)), in particular for changes to the production code ([see factsheet 11 – Managing IT developments](#)).
- **Check the quality of data and annotations, the possible presence of bias, the reliability of data sources**, in particular in order to prevent the data from being manipulated by a third party (e.g. poisoning).
- **Avoid partial or total copies of databases** and restrict access and use of databases only to authorised persons in cases requiring it. **Use fictitious or synthetic data** in other cases, such as security testing, integration, or some audits.
- **Build a documentary collection** for developers and users of the system, including:
 - the design of the system, including the data and models used and the analyses which led to their selection and validation, and the results of those analyses;
 - the operation of the system throughout its life cycle, its performances, the analysis of its biases and the results obtained, its conditions and limitations of use, such as cases where performance may be insufficient;
 - the material equipment necessary for the use of the system, the expected latency or the maximum capacity for systems accessible in SaaS.
- **Verify the legitimacy of users** of the system when it is made available as a service, in order to avoid an attack attempt such as an **attack by model inversion**¹²⁶ or **denial of service**.
- **Provide for an audit plan of the system**, covering software, hardware, and organisational measures such as **procedures for human oversight of the AI system**.

¹²⁶ Les attaques par inversion de modèle visent à reconstituer les données ayant servi pour l'apprentissage du système.

What should be avoided

- Training a model on data **whose source is unknown or unreliable, or whose quality, and in particular the quality of the annotation, has not been verified.**
- Deploying, sharing, disseminating or making accessible a model **without checking the quality of outputs**, and in **particular the absence of problematic outputs** (e.g. hate content) **and personal data**, except for testing and audit purposes.
- Using a system **without knowing its limitations**, or **without assessing the consequences of an error or bias.**

TO GO FURTHER

- The CNIL has published a set of factsheets¹²⁷ on the development phase of AI systems involving personal data.
- The models of attacks on AI systems are diverse and still little known. The CNIL Digital Innovation Laboratory (LINC) has published a first article listing these attacks¹²⁸ as well as a second identifying good security practices to protect themselves¹²⁹ (such as federated learning, or differential privacy).
- The collection of personal data can be minimised by data augmentation or data synthesis techniques, or by focusing the collection on quality data.
- The data used during the deployment phase can change over time, and lose quality for several reasons (e.g.: deterioration of a sensor, drifting or poisoning data). These changes need to be monitored.
- The result provided by the system can be accompanied by information allowing the user to interpret it and identify a possible error (e.g.: confidence score, salience map).
- Measures, such as output filters, reinforcement learning from human feedback (RLHF) or watermarking of generated content, make it possible to secure the content produced by the system.

¹²⁷ "AI how-to sheets", cnil.fr

¹²⁸ "Petite taxonomie des attaques des systèmes d'IA", linc.cnil.fr

¹²⁹ "Sécurité des systèmes d'IA, les gestes qui sauvent", linc.cnil.fr

FACTSHEET 25 – API: APPLICATION PROGRAMMING INTERFACES

Ensure that shared data is secured through the implementation of an API.

The use of application programming interfaces (APIs) is a good practice for many cases of personal data exchange, as APIs can help to make these exchanges more reliable, minimal and secure. To do this, API management must be part of the information systems security policy and be coordinated between API providers and consumers.

Basic precautions

- Identify the actors and their **functional role** (data holder, API manager, re-user¹³⁰) in order to organise the allocation perimeter of each in **terms of access to APIs and data**.
- Limit the sharing to **strictly necessary data**, only to **individuals and for the intended purposes**, in accordance with the principle of minimisation.
- Create a separation between calls to the common functions of the API and those dedicated to its administration, for which robust authentication appears necessary.
- Have **relevant logs** to track exchanges ([see factsheet 16 – Logging operations](#)) and to detect and react in the event of misuse of the API, illegitimate access to data, exceeding access capacity or any other unusual behaviour ([see factsheet 19 – Managing incidents and violations](#)).
- **Keep the documentation up-to-date**. This must include the **format of the queries and data** involved in the sharing in order to limit the risk of a misinterpretation.

What should be avoided

- Keep **old versions of an API active** that do not allow the expected level of security to be maintained.
- Neglect the security of **API access keys**, while secret security solutions, such as a digital safe, exist.

¹³⁰ The data re-user is any organization considering accessing or receiving data through an API for use on its own account.

TO GO FURTHER

- Before the launch of an API, check its resistance to the risks published by the OWASP in its **Top 10 API** ¹³¹.
- See the CNIL ¹³² recommendation on Secure Data Sharing by API.
- The implementation of the API must be in accordance with standard security measures such as the implementation of an **appropriate authentication mechanism** ([see factsheet 4 – Authenticating users](#)), the periodic management of authorisations ([see factsheet 5 – Access management](#)) or the **encryption of communications** at the state of the art.
- A sandbox version of the API should be made available to allow experiments and test the expected results from fictitious data.

¹³¹ "OWASP API Security Top 10", owasp.org

¹³² "API : les recommandations de la CNIL sur le partage de données", cnil.fr

ASSESS THE SECURITY LEVEL OF MY ORGANISATION'S PERSONAL DATA

Have you thought about...

FACTSHEETS		MEASURES	
1	Managing data security	Make security a shared issue and involve management	☐
		Regularly check the effectiveness of technical and organisational measures and adopt a continuous improvement approach	☐
2	Defining a framework for users	Draft an IT charter including procedures for the use of IT equipment and telecommunications resources, the security rules and the means of administration in place	☐
		Give binding force to the charter and remind of the sanctions incurred in the event of non-compliance	☐
3	Involving and training users	Raise awareness among users (both internal and external to the organisation) working with personal data about the privacy risks	☐
		Adapt the content and language of awareness campaigns to the roles of the recipient	☐
4	Authenticating users	Grant a unique identifier to each user	☐
		Adopt a password policy in line with CNIL's recommendations	☐
		Require the user to change the password assigned automatically or by an administrator	☐
5	Access management	Define authorisation profiles	☐
		Withdraw outdated access permissions	☐
		Carry out, at least annually, a review of authorisations	☐
6	Securing workstations	Provide an automatic session locking mechanism	☐
		Install a firewall software	☐
		Use regularly updated antivirus	☐
		Obtain the consent of the user prior to any intervention on his/her position	☐
7	Securing mobile computing	Raise users' awareness regarding risks associated with the use of mobile IT tools	☐
		Implement or integrate an encryption solution for nomadic or removable storage devices	☐
		Require a secret (e.g.: password, pattern) for unlocking smartphones	☐
8	Protecting the computer network	Limit Internet flows to the strict necessary	☐
		Manage Wi-Fi networks, including by implementing the WPA3 protocol	☐
		Enforce VPN use for remote access	☐
		Partition the network, by at least setting up a DMZ (demilitarised zone)	☐
9	Securing servers	Uninstall or disable unnecessary services and interfaces	☐
		Restrict access to administration tools and interfaces only to authorised personnel	☐
		Install critical updates without delay after testing them where appropriate	☐

FICHES		MESURES	
10	Securing websites	Secure data exchange flows	☐
		Ensure that no secrets or personal data are transmitted through URLs	☐
		Check that user entries match what is expected	☐
11	Managing IT developments	Integrate data protection from the design	☐
		Provide privacy-friendly settings by default	☐
		Perform a non-regression test and/or a code review before any update goes to production	☐
		Using fictional or anonymised data for development and testing	☐
12	Protecting the premises	Restrict access to premises by means of locked doors	☐
		Install intrusion alarms and check their proper operation periodically	☐
13	Securing exchanges with the outside world	Encrypt data before transmitting it	☐
		Make sure it's the right recipient	☐
		Ensure confidentiality of secrets by transmitting them via a separate channel	☐
14	Managing data processors	Provide for specific clauses in processors' contracts	☐
		Set out the conditions for the return and destruction of data	☐
		Provide the means to verify the effectiveness of the data protection guarantees	☐
15	Supervising the maintenance and end-of-life of hardware and software	Record maintenance interventions in a log book	☐
		Ensure that third-party interventions are supervised by an organisation manager	☐
		Securely delete the data from equipment before its disposal	☐
16	Logging operations	Provide a logging system	☐
		Inform users about the logging system	☐
		Protect logging equipment and logged information	☐
		Actively analyse logs to detect the occurrence of an incident	☐
17	Saving	Make frequent data backups	☐
		Protect backups, both during storage and transport	☐
		Regularly test the integrity of backups and the ability to restore them	☐

FACTSHEETS		MEASURES
18	Predicting continuity and resumption of activity	Write a business continuity plan and disaster recovery plan ☐
		Regularly perform tests ☐
19	Managing incidents and violations	Process alerts raised by the logging system ☐
		Provide internal procedures and responsibilities for incident management, including for notifying regulators of personal data breaches ☐
20	Risk analysis	Carry out a risk analysis, even a minimal one, on the future data processing ☐
		Ensure that the planned measures are implemented and monitored ☐
		Regularly review the risk analysis ☐
21	Encryption, hash, signature	Use recognised and safe algorithms, software and libraries ☐
		Protect cryptographic secrets and keys ☐
22	Cloud computing	Include cloud services into the risk analysis ☐
		Evaluate the guaranteed level of security set up by the cloud provider ☐
		Make sure security requirements and liability allocation are covered by a contract between the supplier and the customer ☐
		Ensure the same level of security in the cloud as on-premises ☐
23	Mobile applications: Design and development	Consider the specificities of the operating system in order to reduce the personal data collected and limit the permissions requested ☐
		Secure communications by encapsulating them in a TLS channel ☐
		Use cryptographic suites included in the operating system and the hardware protections of secrets ☐
24	Artificial intelligence: Design and learning	Adopt good security practices for development ☐
		Ensure the quality and integrity of data and annotations used for learning and inference ☐
		Provide an audit plan of the system ☐
25	API: Application programming interfaces	Organise and document the allocation perimeter of the API in terms of security and data access ☐
		Limit data sharing to strictly necessary data and to individuals for the intended purposes ☐

CNIL
3, Place de Fontenoy – TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

March 2024

www.cnil.fr
linc.cnil.fr



LICENSE :
www.cnil.fr/mentions-legales