Privacy Impact Assessment (PIA)

KNOWLEDGE BASES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

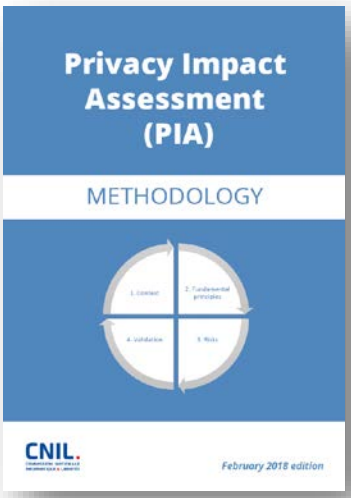
February 2018 edition

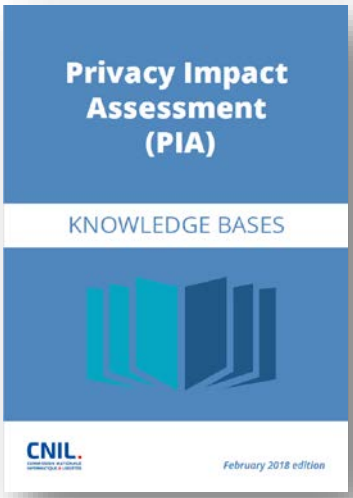
Contents

Foreword

The methodology of the French Data Protection Authority (CNIL) comprises three guides: one setting out the approach, a second containing facts that could be used for formalising the analysis and a third providing knowledge bases (a catalogue of controls aimed at complying with the legal requirements and treating the risks, and examples):

These can be downloaded from the CNIL's website:





https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual

Writing conventions for all of these documents:

- the term "**privacy**" is used as shorthand to refer to all fundamental rights and freedoms (particularly those mentioned in the [GDPR], by Articles 7 and 8 of the [EU Charter] and Article 1 of the [DP-Act]: "privacy, human identity, human rights and individual or public liberties");
- the acronym "**PIA** " is used interchangeably to refer to Privacy Impact Assessment and Data Protection Impact Assessment (DPIA);
- wordings in square brackets ([title]) correspond to references.

1 Knowledge bases for the study

1.1. Typology of personal data

Personal data categories are generally as follows:

Personal data types	Personal data categories
Common personal data	Civil status, identity, identification data
	Personal life (living habits, marital status, etc. –excluding sensitive or dangerous data)
	Professional life (résumé, education and professional training, awards, etc.)
	Economic and financial information (income, financial situation, tax situation, etc.)
	Connection data (IP addresses, event logs, etc.)
	Location data (travels, GPS data, GSM data, etc.)
Personal data perceived as sensitive	Social security number
	Biometric data
	Bank data
Sensitive personal data in the meaning of [DP-Act][1]	Philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, data concerning health or sex life
	Offenses, convictions, security measures

1.2. Typology of personal data supporting assets

Personal data supporting assets are components of the information system on which personal data rely:

Types of personal data supporting assets		Examples
Information systems	Hardware and electronic data media	Computers, communications relays, USB drives, hard drives
	Software	Operating systems, messaging, databases, business applications
	Computer channels	Cables, WiFi, fiber optic
Organizations	People	Users, IT administrators, policymakers
	Paper documents	Prints, photocopies, handwritten documents
	Paper transmission channels	Mail, workflow

1.3. Typology of risk sources

The following table shows examples of risk sources:

[1] See Articles 8 and 9 of [DP-Act] and Article 8 of [Directive-95-46].

Types of risk sources	Examples
Internal human sources	Employees, IT managers, trainees, managers
External human sources	Recipients of personal data, authorized third parties[2], service providers, hackers, visitors, former employees, activists, competitors, customers, maintenance staff, maintenance, offenders, trade unions, journalists, non-governmental organizations, criminal organizations, organizations under the control of a foreign state, terrorist organizations, nearby industrial activities
Non-human sources	Malicious code of unknown origin (viruses, worms, etc.), water (pipelines, waterways, etc.), flammable, corrosive or explosive materials, natural disasters, epidemics, animals

1.4. Typology of the outcomes of feared events

Feared events may have different consequences if they occur:

Feared events	Types of outcomes	Description
Illegitimate access to personal data	None	The data are seen by people who do not need to know them, though these people do not use them.
	Storage	The data are copied and saved to another location without being further used.
	Redistribution	The data are disseminated more than necessary and beyond the control of the data subjects (e.g. unwanted dissemination of a photo on the Internet, loss of control over information published in a social network, etc.)
	Use	The data are used for purposes other than those planned and/or in an unfair manner (e.g. commercial purposes, identity theft, use against data subjects, etc.) or correlated with other information relating to the data subjects (e.g. correlation of residence address and real-time geolocation data, etc.)
Unwanted modification of personal data	Malfunction	The data are modified into valid or invalid data, which will not be used correctly, the processing liable to cause errors, malfunctions, or no longer provide the expected service (e.g. impairing the proper progress of important steps, etc.)
	Use	The data are modified in other valid data, such that the processing operations have been or could be misused (e.g. use to steal identities by changing the relationship between the identity of individuals and the biometric data of other individuals, etc.).
Disappearance of personal data	Malfunction	The data are missing for personal data processings, which generates errors, malfunctions, or provides a different service than the one expected (e.g. some allergies are no longer reported in a medical record, some information contained in tax returns has disappeared, which prevents the calculation of the tax amount, etc.)
	Blockage	The data are missing for personal data processings which can no longer provide the expected service (e.g. slowing down or blocking of administrative or commercial processes, inability to provide care due to the loss of medical records, inability of data subjects to exercise their rights, etc.).

[2] For example, public authorities and court officers may request disclosure of certain data when the law expressly permits them to do so.

1.5. Scales and rules for estimating severity

Severity represents the magnitude of a risk. It is primarily estimated in terms of the extent of potential impacts on data subjects, taking account of existing, planned or additional controls (which should be mentioned as justification).

The following scale can be used to estimate the severity of feared events (**Important: these are only examples, which can be very different depending on the context**):

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[3]	Examples of material impacts[4]	Examples of moral impacts[5]
1. Negligible	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem	- Lack of adequate care for a dependent person (minor, person under guardianship) - Transient headaches	- Loss of time in repeating formalities or waiting for them to be fulfilled - Receipt of unsolicited mail (e.g. spams) - Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing) - Targeted advertising for common consumer products	- Mere annoyance caused by information received or requested - Fear of losing control over one's data - Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion) - Loss of time in configuring one's data - Lack of respect for the freedom of online movement due to the denial of access to a commercial site (e.g. alcohol because of the wrong age)
2. Limited	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	- Minor physical ailments (e.g. minor illness due to disregard of contraindications) - Lack of care leading to a minor but real harm (e.g. disability) - Defamation resulting in physical or psychological retaliation	- Unanticipated payments (e.g. fines imposed erroneously), additional costs (e.g. bank charges, legal fees), payment defaults - Denial of access to administrative services or commercial services - Lost opportunities of comfort (i.e. cancellation of leisure, purchases, holiday, termination of an online account) - Missed career promotion - Blocked online services account (e.g. games, administration) - Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects - Cost rise (e.g. increased insurance prices) - Non-updated data (e.g. position held previously)	- Refusal to continue using information systems (whistleblowing, social networks) - Minor but objective psychological ailments (defamation, reputation) - Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation, loss of recognition) - Feeling of invasion of privacy without irreversible damage - Intimidation on social networks

[3] Loss of amenity, disfigurement, or economic loss related to physical integrity.
[4] Loss incurred or lost revenue with respect to an individual's assets.
[5] Physical or emotional suffering, disfigurement or loss of amenity.

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[3]	Examples of material impacts[4]	Examples of moral impacts[5]
			- Processing of incorrect data creating for example accounts malfunctions (bank, customers, with social organizations, etc.) - Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g. pregnancy advertising, drug treatment) - Inaccurate or inappropriate profiling	
3. Significant	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	- Serious physical ailments causing long-term harm (e.g. worsening of health due to improper care, or disregard of contraindications) - Alteration of physical integrity for example following an assault, an accident at home, work, etc.	- Misappropriation of money not compensated - Non-temporary financial difficulties (e.g. obligation to take a loan) - Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban) - Prohibition on the holding of bank accounts - Damage to property - Loss of housing - Loss of employment - Separation or divorce - Financial loss as a result of a fraud (e.g. after an attempted phishing) - Blocked abroad - Loss of customer data	- Serious psychological ailments (e.g. depression, development of a phobia) - Feeling of invasion of privacy with irreversible damage - Feeling of vulnerability after a summons to court - Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression) - Victim of blackmailing - Cyberbullying and harassment
4. Maximum	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome	- Long-term or permanent physical ailments (e.g. due to disregard of contraindications) - Death (e.g. murder, suicide, fatal accident) - Permanent impairment of physical integrity	- Financial risk - Substantial debts - Inability to work - Inability to relocate - Loss of evidence in the context of litigation - Loss of access to vital infrastructure (water, electricity)	- Long-term or permanent psychological ailments - Criminal penalty - Abduction - Loss of family ties - Inability to sue - Change of administrative status and/or loss of legal autonomy (guardianship)

The value of the level that best matches the potential impacts identified is then selected, by comparing the impacts identified in the context considered with the generic impacts in the scale.

The severity level thus obtained may be raised or lowered by including additional factors:

- level of identification of personal data;
- nature of risk sources;
- number of interconnections (especially with foreign sites);
- number of recipients (which facilitates the correlation between originally separated personal data).

1.6. Scale and rules for estimating likelihood

Likelihood represents the feasibility of a risk to occur. It is primarily estimated in terms of the level of vulnerabilities of the supporting assets concerned and the level of capabilities of the risk sources to exploit them, taking account of existing, planned or additional controls (which should be mentioned as justification).

The following scale can be used to estimate the likelihood of threats:

1. Negligible: it does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
2. Limited: it seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in a room protected by a badge reader).
3. Significant: it seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).
4. Maximum: it seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in the public lobby).

The value of the level that best matches the vulnerabilities of the supporting assets and the risk sources is then selected.

The likelihood level thus obtained may be raised or lowered by including additional factors:

- opening on the Internet or a closed system;
- data exchanges with foreign countries or not;
- interconnections with other systems or no interconnection;
- heterogeneity or homogeneity of the system;
- variability or stability of the system;
- the organization's image.

1.7. Threats that can lead to an illegitimate access to personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
C	Hardware	Used inappropriately	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, the hard drive containing the information is used for purposes other than the intended purpose (e.g. to transport other data to a service provider, to transfer other data from one database to another, etc.)	Usable for other than the intended purpose, disproportion between hardware capacities and the required capacities (e.g. hard drive of several TB to store few GB of data)
C	Hardware	Observed	Watching a person's screen without their knowledge while on the train; taking a photo of a screen; geolocation of hardware; remote detection of electromagnetic signals	Allows interpretable data to be observed; generates compromising emanations
C	Hardware	Altered	Tracking by a hardware-based keylogger; removal of hardware components; connection of devices (such as USB flash drives) to launch an operating system or retrieve data	Allows components (boards, expansion cards) to be added, removed or substituted via connectors (ports, slots); allows

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
				components to be disabled (USB port)
C	Hardware	Lost	Theft of a laptop from a hotel room; theft of a work cell phone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device	Small, appealing targets (market value)
C	Software	Used inappropriately	Content scanning; illegitimate cross-referencing of data; raising of privileges, erasure of tracks; sending of spam via an e-mail program; misuse of network functions	Makes data accessible for viewing or manipulation (deletion, modification, movement); may be used for other than normal purposes; allows the use of advanced functionalities
C	Software	Observed	Scanning of network addresses and ports; collection of configuration data; analysis of source codes in order to locate exploitable flaws; testing of how databases respond to malicious queries	Possibility of observing the functioning of software; access to and reading of source codes
C	Software	Altered	Tracking by a software-based key logger; infection by malicious code; installation of a remote administration tool; substitution of components during an update, a maintenance operation or installation (code-bits or applications are installed or replaced)	Editable (improvable, configurable); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources); does not function properly or as expected
C	Computer channels	Observed	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network	Permeable (generation of compromising emanations); allows interpretable data to be observed
C	People	Observed	Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings	People who cannot keep things to themselves, are predictable (with routine lives that make repeated espionage easy)
C	People	Manipulated	Influence (phishing, social engineering, bribery), pressure (blackmail, psychological harassment)	Easily influenced (naive, gullible, obtuse, low self-esteem, little loyalty), easily manipulated (vulnerable to pressure placed on themselves or their circle of family and friends)
C	People	Lost	Employee poaching; assignment changes; takeover of all or part of the organization	Little loyalty to the organization; personal needs that are largely unmet; easy breach of contractual obligations
C	Paper documents	Observed	Reading, photocopying, photographing	Allows interpretable data to be seen
C	Paper documents	Lost	Theft of files from offices; theft of mail from mailboxes; retrieval of discarded documents	Portable
C	Paper transmission channels	Observed	Reading of signature books in circulation; reproduction of documents in transit	Observable

1.8. Threats that can lead to an unwanted modification of personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
I	Hardware	Altered	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of an application	Allows components (boards, expansion cards) to be added, removed or substituted via connectors (ports, slots); allows components to be disabled (USB port)
I	Software	Used inappropriately	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data	Makes data accessible for viewing or manipulation (deletion, modification, movement); may be used for other than normal purposes; allows the use of advanced functionalities
I	Software	Altered	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components	Editable (improvable, configurable); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources); does not function properly or as expected
I	Computer channels	Used inappropriately	Man-in-the-middle attack to modify or add data to network traffic; replay attack (resending of intercepted data)	Allows traffic to be altered (interception then resending of data, possibly altered); sole means of transmission for the flow; allows the computer channel-sharing rules to be changed (transmission protocol authorizing the addition of nodes)
I	People	Overloaded	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills	Insufficient resources for assigned tasks; capacities not suited to working conditions; insufficient skills for carrying out duties Inability to adapt to change
I	People	Manipulated	Influence (rumor, disinformation)	Easily influenced (naive, gullible, obtuse)
I	Paper documents	Altered	Changes to figures in a file; replacement of an original by a forgery	Falsifiable (paper documents with editable content)
I	Paper transmission channels	Altered	Changes to a memo without the author's knowledge; change from one signature book to another; sending of multiple conflicting documents	Allows distributed documents to be altered; sole means of transmission for the channel; allows the paper transmission channel to be altered

1.9. Threats that can lead to a disappearance of personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
D	Hardware	Used inappropriately	Storage of personal files; personal use	Usable for purposes other than the intended purpose
D	Hardware	Overloaded	Storage unit full; power outage; processing capacity overload; overheating; excessive temperatures, denial of service attack	Storage capacities too low; processing capacities too low and not adapted to the processing conditions; constant electricity supply required for operation; sensitive to voltage variations

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
D	Hardware	Altered	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of the system	Allows components (boards, expansion cards) to be added, removed or substituted via connectors (ports, slots); allows components to be disabled (USB port)
D	Hardware	Damaged	Flooding, fire, vandalism, damage from natural wear and tear, storage device malfunction	Poor-quality components (fragile, easily flammable, poor aging resistance); not suited to the conditions of use; erasable (vulnerable to magnetic fields or vibrations)
D	Hardware	Lost	Theft of a laptop, loss of a cell phone; disposal of a supporting asset or hardware, under-capacity drives leading to a multiplication of supporting assets and to the loss of some	Portable, appealing targets (market value)
D	Software	Used inappropriately	Erasure of data; use of counterfeit or copied software; operator errors that delete data	Makes data accessible for viewing or manipulation (deletion, modification, movement); may be used for other than normal purposes; allows the use of advanced functionalities
D	Software	Overloaded	Exceeding of database size; injection of data outside the normal range of values, denial of service attack	Allows any kind of data to be entered; allows any volume of data to be entered; allows actions to be executed using input data; low interoperability
D	Software	Altered	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components	Editable (improvable, configurable); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources); does not function properly or as expected
D	Software	Damaged	Erasure of a running executable or source codes; logic bomb	Possibility of erasing or deleting programs; sole copy; complex in terms of use (not very user-friendly, few explanations)
D	Software	Lost	Non-renewal of the license for software used to access data, stoppage of security maintenance updates by the publisher, bankruptcy of the publisher, corruption of storage module containing the license numbers	Sole copy (of license agreements or software, developed internally.); appealing (rare, innovative, high commercial value.); transferable (full transfer clause in license)
D	Computer channels	Overloaded	Misuse of bandwidth; unauthorized downloading; loss of Internet connection	Non-scalable transmission capacities (insufficient bandwidth; limited amount of telephone numbers)
D	Computer channels	Damaged	Cut wiring, poor Wi-Fi reception, corrosion of cables	Alterable (fragile, breakable, poor cable structure, bare cables, disproportionate sheath), sole
D	Computer channels	Lost	Theft of copper cables	Appealing targets (market value of cables), transportable (lightweight, may be hidden); inconspicuous (easily forgotten, trivial, do not stand out)
D	People	Overloaded	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills	Insufficient resources for assigned tasks; capacities not suited to working conditions; insufficient

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
				skills for carrying out duties; inability to adapt to change
D	People	Damaged	Occupational accident; occupational disease; other injury or disease; death; neurological, psychological or psychiatric ailment	Physical, psychological or mental limits
D	People	Lost	Death, retirement, reassignment; contract termination or dismissal; takeover of all or part of the organization	Little loyalty to the organization; personal needs that are largely unmet; easy breach of contractual obligations
D	Paper documents	Used inappropriately	Gradual erasure over time; voluntary erasure of portions of a document, reuse of paper to take notes not related to the processing, to make a shopping list, use of notebooks for something else	Editable (paper document with erasable content, thermal papers not resistant to temperature changes)
D	Paper documents	Damaged	Aging of archived documents; burning of files during a fire	Poor-quality components (fragile, easily flammable, poor aging resistance); not suited to the conditions of use
D	Paper documents	Lost	Theft of documents; loss of files during a move; disposal	Portable
D	Paper transmission channels	Overloaded	Mail overload; overburdened validation process	Existence of quantitative or qualitative limits
D	Paper transmission channels	Damaged	End of workflow following a reorganization; mail delivery halted by a strike	Unstable, sole
D	Paper transmission channels	Altered	Change in how mail is sent; reassignment of offices or premises; reorganization of paper transmission channels; change in working language	Editable (replaceable)
D	Paper transmission channels	Lost	Elimination of a process following a reorganization; loss of a document delivery company, vacancy	Unrecognized need

1.10. Scales for the action plan

The scales below can be used to develop the action plan and monitor its implementation:

Criteria	Level 1	Level 2	Level 3
Difficulty	Low	Moderate	High
Financial cost	Nil	Moderate	High
Term	Quarter	Year	3 years
Progress	Not started	In progress	Completed

2 Anonymization

Aims: to remove identifying characteristics from personal data.

Good practices to be followed if the measure is used to address risks

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

3 Archiving

Aims: to define all procedures for preserving and managing the electronic archives containing the personal data intended to ensure their value (specifically, their legal value) throughout the entire period necessary (transfer, storage, migration, accessibility, elimination, archiving policy, protection of confidentiality, etc.).

Good practices to be followed if the measure is used to address risks

- Confirm that the archive management processes are defined.
  - ♦ *Recommendations: distinguish the transfer, storage, management of descriptive data, consultation/communication and administration processes (relationship with the offices of origin, technological and legal monitoring, upgrade and migration of media and formats).*
- Confirm that the archiving roles are identified.
  - ♦ *Recommendations: distinguish the offices of origin, transferring agencies, archiving authorities (responsible for preservation) and inspection agencies (exercising scientific and technical control over the public archives).*
- Confirm that the measures can ensure, if necessary, the identification and authentication of the origin of the archives, integrity, intelligibility, readability, availability and accessibility of the archives, how long the archives must be kept and the traceability of the operations carried out on the archives (including transfer, consultation, migration, deletion, etc.) and take additional measures if this is not the case.
  - ♦ *Recommendations: implement access methods specific to the archived data, encrypt the archives and prepare to re-encrypt them securely with new keys before the end of life of the encryption keys, prepare to change obsolete data supporting assets; choose a procedure ensuring that the entire archive has been destroyed.*
- Determine the methods for protecting the confidentiality of the archived personal data based on the risks identified.
  - ♦ *Recommendations: systematically encrypt the sensitive data (in the meaning of Article 8 and data coming under Article 9 of the Data Protection Act (DP-Act)) archived.*
- Confirm that the archive authorities have an archiving policy (AP).
  - ♦ *Recommendations: the AP document should formally document the legal, functional, operational and technical restrictions that the various stakeholders must comply with so that the electronic archiving established can be considered reliable and permanent.*
- Confirm that a declaration of archiving practices (DAP) exists.
  - ♦ *Recommendations: the DAP document should describe all procedures established to achieve the objectives set forth in the archiving policy.*

Tools/ To find out more

- See the forthcoming ANSSI-Archiving guide and the NF-42-013 standard.
- See the Archives de France site.

4 Encryption

4.1 General measures

Aims: to make personal data unintelligible to anyone without access authorization (symmetric or asymmetric encryption, use of public algorithms known to be strong, authentication certificate, etc.).

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- See the requirements regarding the General Security Framework (RGS), "Confidentiality" function.

4.2 Specific measures for symmetric encryption

Good practices to be followed if the measure is used to address risks

- Only use a key for a single purpose.
- Choose a mechanism that is recognized by the appropriate organizations.
    - ♦ *Recommendations: use mechanisms that comply with the RGS, such as the AES algorithm, use a processed block size equal to at least 128 bits, a non-deterministic encryption scheme (such as a CBC mechanism with a random initialization vector), cryptographic keys of a length appropriate to the expected useful life (for example, at least 128 bits for confidentiality guaranteed until 2020) and which are not weak keys, etc.*
- Formally document the key management system.
    - ♦ *Recommendations: draft a procedure.*

4.3 Specific measures for asymmetric (public key) encryption

Good practices to be followed if the measure is used to address risks

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

4.4 Specific measures for encrypting equipment

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

Good practices to be followed if the measure is used to address risks

- Encrypt data at the hardware level (surface of the hard disk) or at the operating system level (encryption of a partition or a container).

♦ *Recommendations: use encryptable equipment, such as hard disks with SED technology or software such as dm-crypt (Linux), FileVault (MacOS), VeraCrypt (Windows).*

- Choose systems that do not store keys on the equipment that will be encrypted unless this implements a secure storage device (such as a TPM chip for laptops).

4.5 Specific measures for encrypting databases

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

Good practices to be followed if the measure is used to address risks

• Based on the risks identified, encrypt the storage area (at the level of the hardware, operating system or database) so as to provide protection from physical theft, of the piece of data itself (encryption by application), with a view to guaranteeing the confidentiality of certain data as regards the administrators themselves. In the event of partitioned IT teams, database encryption can make data accessible only to database administrators, to the exclusion of system administrators.

4.6 Specific measures for encrypting partitions or containers

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

Good practices to be followed if the measure is used to address risks

• Encrypt the data at operating system level (encryption of a partition, directory or file) or using specialized software (encryption of a container).

♦ *Recommendations*: *use software such as VeraCrypt or Zed!.*

4.7 Specific measures for encrypting standalone files

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

Good practices to be followed if the measure is used to address risks

• Encrypt the stored files or the email attachments.

♦ *Recommendations*: *use such software as ZoneCentral, those using the Security BOX Crypto 6.0 library, or AxCrypt or Gnu Privacy Guard (GPG)*

for example. Otherwise, use at least a compression tool that allows encryption with a password, such as 7-Zip, which provides AES encryption, or an equipment solution such as a Bull Trustway PCI cryptographic card, etc.

4.8 Specific measures for encrypting email

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

Good practices to be followed if the measure is used to address risks

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

4.9 Specific measures for encrypting a communications channel

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

Good practices to be followed if the measure is used to address risks

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

5 Data partitioning (in relation to the rest of the information system)

Aims: to reduce the possibility of personal data being correlated and of a blanket data breach occurring (identify the datasets specific to each business and separate them in logical fashion, etc.).

Good practices to be followed if the measure is used to address risks

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

6 Physical access control

Aims: to limit the risks that unauthorized persons will gain physical access to personal data (list of authorized persons, authentication of staff and visitors, a record of access granted, warning in the event of unauthorized entry, etc.).

Good practices to be followed if the measure is used to address risks

- Categorize areas of the buildings by risk.
  - ♦ *Recommendations: delimit an area open to the public when the organization has a functional duty to greet the public (reception counter, waiting room or meeting room), an area assigned to the service (a controlled-access area corresponding to the offices where data are processed) and a security area (housing the servers, network administration stations, the network's active components or sensitive resources such as energy supply and distribution equipment or network and telephony equipment).*
- Maintain an up-to-date list of individuals (including visitors, employees, authorized employees, trainees and service providers) who are authorized to enter each area.
  - ♦ *Recommendations: review access rights to the security areas regularly and delete them if necessary.*
- Select methods for authenticating employees that are proportional to the risks associated with each area.
  - ♦ *Recommendations: if the risks are low, one person stationed at the reception area is sufficient to identify employees; if they are higher (restricted or security area), an access gate or other form of access control with a proximity badge showing the wearer's identification photograph and/or employee identification number is recommended; the badge should be visible.*
- Select visitor authentication methods (for example, persons coming to attend a meeting, external service providers or auditors) proportional to the risks associated with each area.
  - ♦ *Recommendations: if the risks are low, authentication may not be necessary; however, if they are high, establish a reception policy for outside visitors based on a predefined schedule, confirm their identification and provide a badge that is valid only for the length of their visit.*
- Define actions to take if authentication fails (identity cannot be confirmed or lack of authorization to enter a security area).
  - ♦ *Recommendations: deny entry to the visitor and notify the person in charge of security, etc.*
- Keep a record of access granted after notifying the data subjects.
  - ♦ *Recommendations: record visitors' identity, date and time of arrival and departure, maintain an access log dating back no more than three months.*

- Visitors needing to access premises outside public reception areas should be escorted (from the time they arrive, during their visit and until they exit the premises) by a member of the organization.
- Protect the most sensitive areas in proportion to the risks.
    - ♦ *Recommendations: install a locked door, digital code or videophone; renew the means of access on a regular basis (door entry codes); identify the area with clear, visible signage that can be understood by all visitors; secure the openings (window bars for ground floor and lower floor premises or reinforced doors with an access control system).*
- Install a warning system in the event of unauthorized entry.
    - ♦ *Recommendations: install systems that detect openings and unauthorized entries and that transmit a centralized warning (on-site security and outsourced services), particularly in security areas, and monitor the most sensitive areas using a CCTV system.*

Tools/To find out more

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

7 Integrity monitoring

7.1 General measures

Aims: to be warned in the event of an unwanted modification or disappearance of personal data (hash function, message authentication code, electronic signature, preventing SQL injections, etc.).

Good practices to be followed if the measure is used to address risks

- Identify the data that must be monitored for integrity based on the risks identified.
- Choose a method for monitoring their integrity based on the context, the risks assessed and the robustness required.
  - ♦ *Recommendations: use a hash function to generate a fingerprint (hash) of the data to address the risks related to errors; apply a message authentication code (MAC) to address the risks related to errors and modification by any person unfamiliar with the key; apply an electronic signature function to address the risks related to errors and modification by anyone other than the signatory.*
- Determine when the function is to be applied and when the monitoring should be performed based on implementation of the business process.
  - ♦ *Recommendations: to monitor the integrity of the data at every use, each piece of data may be fingerprinted when entered, another fingerprint may be taken each time the data are displayed and a visual warning may appear if they do not match (in which case, the data can be restored if they were backed up previously), etc.*
- When the data are sent to a database, analytical measures must be set up to prevent scripting or SQL injection attacks.
  - ♦ *Recommendations: prevent the entry of any data (special characters, SQL statements, etc.), filter or encrypt the data before they are saved, limit the volume of data that can be input.*

7.2 Specific measures for a hash function

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

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

7.3 Specific measures for a message authentication code

Good practices to be followed if the measure is used to address risks

• Choose a mechanism recognized by the appropriate organizations and that provides security proof.

♦ *Recommendations: use an algorithm to calculate a message authentication code that complies with the RGS, such as the "retail" CBC-MAC using the AES as a block encryption mechanism and two separate keys (one for the CBC chain and the other for "retail" superencryption).*

7.4 Specific measures for an electronic signature function

Good practices to be followed if the measure is used to address risks

- Only use a key for a single purpose.
- Adopt signature solutions based on public algorithms known to be strong.
  - ♦ *Recommendations: use tools (signature creation devices, signature creation application et signature verification module) that are certified, qualified or subject to first-level security certification by ANSSI at the level corresponding to the robustness expected.*
- Choose a mechanism recognized by the appropriate organizations and that provides security proof.
  - ♦ *Recommendations: use mechanisms that comply with the RGS, such as RSA-SSA-PSS or ECDSA, using one of the P-256, P-384, P-521, B-283, B-409 or B-571 curves.*
- Generate the keys pursuant to the RGS.
  - ♦ *Recommendations: use the services of a registered electronic certificate service provider as specified in version 2 of the RGS for using signatures.*
- Establish mechanisms for verifying the electronic certificates.
  - ♦ *Recommendations: when an electronic certificate is received, verify, at a minimum, that it includes an indication of purpose consistent with expectations, that it is valid and has not been revoked and that a proper chain of certification exists at all levels.*
- Protect the security of key generation and use consistent with their level in the key hierarchy.
- Formally document the key management system.
  - ♦ *Recommendations: develop a "certification policy" (CP) that specifies responsibilities, identification and authentication, certificate life-cycle operational requirements, non-technical and technical security measures, certificate and revocation list profiles and compliance audits and other evaluations.*

Tools/ To find out more

- See the RGS requirements regarding the "Electronic Signature" function.

Notes

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

8 Logical access control

Aims: to limit the risks that unauthorized persons will access personal data electronically (management of user profiles, authentication mechanism, password policy, etc.).

8.1 Managing users' privileges to access personal data

Good practices to be followed if the measure is used to address risks

- Manage users' profiles by separating tasks and areas of responsibility (preferably in centralized fashion) to limit access to personal data exclusively to authorized users by applying need-to-know and least-privilege principles.
    - ♦ *Recommendations: define one or more user profiles in centralized fashion (with specific privileges for the use of functions and creation, access, modification, transfer and deletion of data) and assign each person one of the defined profiles when the employment contract takes effect or upon changing jobs.*
- Identify every person with legitimate access to personal data (employees, contracting parties and other third parties) by a unique identifier.
- If the use of generic or shared identifiers cannot be avoided, obtain validation from top management and implement methods for tracing the use of this kind of identifier.
    - ♦ *Recommendations: fill out an attendance record, complete a register of activities.*
- Limit access to the tools and administration interfaces to authorized persons.
- Limit the use of accounts that provide elevated privileges to operations that require them.
- Limit the use of "administrator" accounts to the IT department and to administration actions that require them.
    - ♦ *Recommendations: "administrator" accounts must be limited to administration tasks; administrators must use an account with more limited rights when they perform actions that are more exposed (for example, reading email or checking the Internet, etc.)*
- Every account, particularly if it has elevated privileges (for example, an administrator account), must have its own password.
    - ♦ *Recommendations: to the extent possible, "administrator" accounts must be individual and require a personal password.*
- Log information connected to the use of privileges (see the page Traceability (logging)).
- Conduct an annual review of privileges to identify and delete unused accounts and to realign the privileges with each user's functions.

- Withdraw the rights of employees, contracting parties and other third parties when they are no longer authorized to access a premises or a resource or when their employment contract ends, and adjust the rights in the event of a job transfer.
  For individuals with a temporary account (including interns and service providers), configure an expiration date when the account is established.

8.2 Authenticate individuals who want to access personal data

Good practices to be followed if the measure is used to address risks

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

Notes

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

Tools/ To find out more

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

8.3 Specific measures for electronic certificate authentication

Good practices to be followed if the measure is used to address risks

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

8.4 Managing the credentials

Good practices to be followed if the measure is used to address risks

- Adopt a password policy, implement it and monitor it automatically to the extent that applications and resources allow, and inform users about it.
    - ♦ *Recommendations: passwords shall be composed of a minimum of eight characters; must be renewed if there is the least concern that they may have been compromised and, possibly, periodically (every six months or once a year) and must include a minimum of three of the four kinds of characters (capital letters, lower case letters, numerals and special characters); when a password is changed, the last five passwords may not be reused; the same password should not be used for different accesses; passwords should not be related to one's personal information (including name or date of birth).*
- Adopt a specific password policy for administrators, implement it and monitor it automatically to the extent that the applications and resources allow, and inform administrators of it.
    - ♦ *Recommendations: passwords must comply with Deliberation no. 2017-012 of January 19, 2017. Moreover, never use the same password for different accesses; passwords should not be related to one's personal information (including name or date of birth); configure the software so that it never retains passwords; define a maximum number of attempts beyond which a warning is issued and authentication is blocked (temporarily or until it is manually unblocked).*
- Immediately change default passwords after installing an application or a system.
- Create an initial unique random password for each user account, transmit it securely to the user, for example by using two separate channels (paper and others) or a scratch-off field, and require that it be changed when the first connection is made and when the user receives a new password (for example, if the old password is forgotten).
- Store the authentication information (including passwords for accessing information systems and private keys linked to electronic certificates) so that it is accessible only to authorized users.
    - ♦ *Recommendations: limit access rights (including reading and writing) to the absolute minimum and encrypt the files in which the passwords are stored.* Sequester the credentials used to administer the IT system resources and keep them updated in a safe or locked cabinet.
- If many passwords or secrets (including private keys and certificates) must be used, implement a centralized authentication solution using OTPs or secure vaults.
    - ♦ *Recommendations: access control based, at a minimum, on a robust master password; secure storage of passwords ensuring that the protected passwords cannot be recovered without knowing the secret (including encryption and masking); secure display of passwords (masking of passwords in login boxes); resistance to attack (including decryption, brute force and replay); automatic closure or blockage (including after a certain period of time or during secure standby).*

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

Notes

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

Tools/To find out more

- See the CERTA-Passwords briefing note.

9 Storage durations: limited

Aims: to comply with Articles 6 and 36 of the DP-Act and Article 5.1(e) of the General Data Protection Regulation (GDPR); to reduce the severity of risks by ensuring that personal data are not retained for longer than necessary.

Good practices

- Define, for each data category, storage durations that are time-limited and appropriate to the purpose of the processing and/or legal requirements.
  - ♦ *Recommendations: define storage durations that are appropriate for each type of data processed; distinguish common data, archived data (access to which is limited to the stakeholders concerned only), functional traces, logs.*
- Check that the processing enables the end of the storage duration to be detected (set up an automatic mechanism based on the date on which the data are created or last used).
  - ♦ *Recommendations: the processing should incorporate the date when each piece of data will or should be deleted.*
- Confirm that the processing allows the deletion of personal data when the storage duration expires and that the method chosen to delete them is appropriate to the risks to the freedoms and privacy of the data subjects.
  - ♦ *Recommendations:* Deletion of a piece of data reaching the end of its storage duration cannot be in a logical fashion (progress indicator specifying that the piece of data has been deleted but can still be read directly in the database).
  - ♦ A good practice may entail defining an intermediate storage duration whereby data are only made accessible to everyone for a certain period of time, and then, beyond a certain timeframe, to a restricted list of persons (e.g. the piece of data is accessible to everyone for 6 months, and then only to the disputes department).
- Once the storage duration has expired, subject to intermediate archiving of the necessary data, delete the data with immediate effect (also see the page Data minimization: adequate, relevant and limited).
  - ♦ *Recommendations: develop an automated functionality that archives/erases personal data when their storage duration expires, including for logs and traces.*
    If deletion is carried out manually, the tool must provide the user with a batch deletion function.
  - ♦ *Where applicable, context-permitting, the storage duration for a piece of data may be extended by the user. By default, the piece of data is deleted at the end of the initially planned duration.*

Notes

- In general, the purpose of the processing does not justify retaining personal data in anticipation of police or court action for a period longer than provided for in the DP-Act and GDPR. However, certain sectors are required to retain certain data for a defined period (for example, telecommunications operators and airline passengers).
- By reducing the amount of available and processed data, archiving and wiping help to limit the impacts in the event of theft or accidental dissemination of the database.

10 Keeping risk sources at a safe distance

Aims: to avoid that risk sources – which may or may not be human – adversely affect personal data (dangerous products, dangerous geographic areas, transfer of data outside the EU, etc.).

Good practices to be followed if the measure is used to address risks

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

11 Exercising the rights to restriction of processing and to object

11.1 General measures

Aims: to comply with Article 38 of the DP-Act and Articles 18 and 21 of the GDPR: to ensure that individuals have an opportunity to object to the use of their personal data; to allow the data subject to call for processing of his/her data to be "frozen", as a protective control while its legitimacy is being checked, for example; to confirm that the processing is not covered by an exception in Article 38 of the DP-Act (legal requirement or exclusion noted in the act establishing the processing) and Article 21 of the GDPR (compelling legitimate grounds, legal rights, public interest) prohibiting the person from objecting to the processing.

Good practices

- Determine the practical means that will be implemented to allow individuals to exercise the right to object. Individuals must be able to exercise this right as quickly as possible, within two months without exception, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the data subjects and must not involve any cost to them.
- Ensure that the right to object may always be exercised and that the personal data collected and processed actually allow the exercise of the right to object.
    - ♦ *Recommendations: analyze the cases in which the practical means chosen are no longer operational and identify backup solutions, if necessary.*
- Ensure that "the interested party is able to express his or her choice prior to the final validation of his or her responses," pursuant to Article 96 of the DP-Act.
    - ♦ *Recommendations: confirm that the right to object may be exercised before the data subjects provide final validation of their responses or before the collection is completed.*
- Confirm that requests to exercise the right to object submitted on-site provide for verification of the identity of the individuals submitting requests and the identity of the individuals they may appoint as their representative.
- Confirm that requests to exercise the right to object submitted by regular mail are signed and accompanied by a photocopy of a piece of identification (which should not be retained unless proof must be kept) and that they specify a reply-to address.
- Confirm that requests to exercise the right to object submitted by email (using an encrypted channel if transmitted via the Internet) include a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file).
- Ensure that individuals exercising their right to object provide legitimate grounds and that those grounds are evaluated (except in the case of marketing and processing for the purpose of health research falling under Chapter IX of the DP-Act, which provides the individual a discretionary right to object).
- Ensure that all recipients of the processing are notified of the objections submitted by the data subjects, pursuant to Article 97 of the DP-Decree.

Notes

- The right to restriction allows the data subject to call for processing of his/her data to be frozen, as a protective control while its legitimacy is being checked, for example.

11.2 Specific measures for processing via telephone

Good practices

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

11.3 Specific measures for processing via electronic form

Good practices

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

11.4 Specific measures for processing via email

Good practices

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

11.5 Specific measures for processing via a connected object or mobile app

Good practices

- Existence of "Privacy" settings.
  - ♦ *Recommendations: give the user the opportunity to change the default settings; makes these settings accessible when the device or app is first activated, and then at any time via a specific menu.*
- Allow the user to object to the collection of special data.

- ♦ *Recommendations: warn the user (icon, light) when the app is running in the background, when the device "is listening" with the microphone, when the location is being collected, etc. and enable the user to object thereto.*

- Take underage users into account.
  - ♦ *Recommendations: recommend a parental control device, exclude children under 13 years of age from any automated profiling processing.*
- Properly stop any collection of data where the user withdraws his/her consent.

11.6 Specific measures for research using identifiable biological samples (i.e. DNA)

Good practices

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

12 Exercising the rights to rectification and erasure

12.1 General measures

Aims: to comply with Article 40 of the DP-Act and Articles 16, 17 and 19 of the General Data Protection Regulation (GDPR); to ensure that individuals may correct, add to, update, block or delete their personal data; to confirm that the processing is not covered by an exception in Article 41 of the DP-Act (national security, defense or public safety) or Article 17 of the GDPR (right of freedom of expression and information, legal obligation, public interest, public health, scientific or historical research purposes or statistical purposes, legal claims).

Good practices

- Determine the practical means that will be implemented to permit the exercise of the right to rectification. Individuals must be able to exercise this right as quickly as possible, within two months without exception, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the data subjects and must not involve any cost to them.
- Ensure that the right to rectification may always be exercised.
    - ♦ *Recommendations: analyze the cases in which the practical means chosen are no longer operational and identify backup solutions, if necessary.*
- Ensure that the right to rectification may always be exercised.
    - ♦ *Recommendations: clear indications and simple steps for erasing data if selling the device or before scrapping it; possibility of erasing the data in the event the device is stolen.*
- Ensure that the identity of individuals submitting requests will be verified.
    - ♦ *Recommendations: confirm that requests to exercise the right to correct submitted via postal mail are signed and accompanied by a photocopy of a piece of identification (which shall not be retained unless proof must be kept), and that requests submitted via email (using an encrypted channel if transmitted via the Internet) are accompanied by a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file) and that requests specify a reply-to address and confirm the identity of individuals submitting requests on-site and of individuals they may appoint as their representatives or of heirs of a deceased individual, etc.*
- Ensure that the accuracy of the corrections requested will be verified.
- Ensure that the data to be deleted are properly erased.
- Ensure that the individuals submitting requests receive confirmation.
- Ensure that the third parties to whom the data may have been sent are informed of the corrections made.
- Upon receiving an erasure request, inform the user if the personal data are going to be kept all the same (technical requirements, legal obligations.)
- Implementing the right to be forgotten for minors.

♦ *An Internet user under 18 years of age can, upon publication or creation of an online account, directly and without the need for an explanation, ask the website to erase data concerning him/her at the earliest possible opportunity. There are exceptions, particularly in the event the information published is necessary for the freedom of information, on the grounds of public interest or to comply with a legal obligation.*

Tools/To find out more

- See Articles 92 to 95 and 99 to 100 of the DP-Act.

Notes

- The data controller has one month in which to erase the data or respond to the data subject. Beyond this time limit, the data subject can refer the case to the CNIL. There are exceptions, particularly in the event the information published is necessary for the freedom of information, on the grounds of public interest or to comply with a legal obligation.
- An Internet user under 18 years of age can, upon publication or creation of an online account, directly and without the need for an explanation, ask the website to erase data concerning him/her at the earliest possible opportunity.

12.2 Specific measures for online targeted advertising

Good practices

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

13 Exercising the right of access and right to data portability

13.1 General measures

Aims: to comply with Article 40 of the DP-Act and Articles 15 and 20 of the General Data Protection Regulation (GDPR); to ensure that individuals have an opportunity to know about their personal data, to enable the user to retrieve, in an easily reusable format, personal data s/he has provided, so as to transfer them to another service; confirm that the processing is not covered by an exception in Articles 39 and 41 of the DP-Act (such as data processed for statistical or research purposes when there is no risk of a privacy breach and the data are retained only as long as necessary for these purposes or for reasons of national security, defense or public safety) and in Article 20 of the GDPR (no portability for processing in the public interest or in the exercise of official authority or respect for the rights and freedoms of others).

Good practices

- Determine the practical means that will be implemented to allow the exercise of the right of access. Individuals must be able to exercise this right as quickly as possible, within two months without exception (one month under the GDPR) for data, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the data subjects and they must not incur expenses that exceed copying costs.
    - ♦ *Recommendations: establish a process to inform individuals submitting requests about the status of their request and the necessary processing (for example, by regular mail or email, noting that the request has been received and the date by which they can expect to receive a response). In the case of stored archives, there may be some leeway regarding the response date if the data controller informs the individual submitting the request of the problems and has provided a reasonable response time.*
- Ensure that the right of access can always be exercised.
    - ♦ *Recommendations: analyze the cases in which the practical means chosen are no longer operational and identify backup solutions, if necessary.*
- Confirm that requests to exercise the right of access submitted on-site provide the identity of the individuals submitting requests and the identity of the individuals they may appoint as their representative.
- Confirm that requests to exercise the right of access submitted by regular mail are signed and accompanied by a photocopy of a piece of identification (which should not be retained unless proof must be kept) and that they specify a reply-to address.
- Confirm that requests to exercise the right of access submitted by email (using an encrypted channel if transmitted via the Internet) are accompanied by a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file).
- Ensure that all information that data subjects may request can be provided while still protecting the personal data of third parties.

Tools/To find out more

- See Articles 92 to 95 and 98 of the DP-Act.
- See the CNIL-Employers guide.

13.2 Specific measures for accessing medical files

Good practices

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

Tools/To find out more

- See Decree-2002-637.

14 Purposes: specified, explicit and legitimate

Aims: to comply with Article 6 of the DP-Act and Article 5.1(b) of the GDPR; to prevent incompatible uses and misuse.

Good practices

- Describe the data processing purposes in detail and justify their legitimacy.
- Explain the purposes of sharing with third parties as well as the data processing purposes for improving the service.
- Explain the specific conditions under which the processing will take place, particularly by clarifying data matching where applicable.

15 Basis: lawfulness of processing, prohibition of misuse

Aims: to comply with Article 6 of the General Data Protection Regulation (GDPR).

Good practices

• Determine and justify the lawfulness criterion applicable to the data processing under consideration:

- ♦ the data subject has consented to the processing of his or her personal data for one or more specific purposes;
- ♦ the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- ♦ the processing is necessary for compliance with a legal obligation to which the controller is subject;
- ♦ the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- ♦ the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- ♦ the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Notes

- where processing is carried out in accordance with a legal obligation or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, clarify in the justification the legal basis for the processing in Union law or the law of the Member State to which the controller is subject.
- There can be several types of basis for a processing operation: for example, a contract associated with the purchase of a product for using it for its primary purpose and consent for its secondary purposes (improving the service, marketing) which will be obtained when the product is activated.
- NB: Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
  - ♦ any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

16 Prior formalities

Aims: to comply with the obligations regarding formalities prior to data processing.

Good practices

- Declare the processing to the CNIL prior to implementing the processing.
- Check that the data processing does indeed comply with the declared purpose.
- Perform a Privacy Impact Assessment (PIA) and have it validated.
- Consult the CNIL if the residual risks are high, pursuant to Article 36 of the General Data Protection Regulation (GDPR).
- Carry out the other sectoral and contractual formalities applicable to the processing (e.g. formalities associated with other codes and regulations, contract with an external data source, etc.)

Tools/To find out more

- See the PIA method and PIA guides of the CNIL.
- See the WP29 guidelines on PIA.

17 Management of incidents and data breaches

Aims: to have an operational organization that can detect and address incidents that may affect the data subjects' freedoms and privacy (definition of responsibilities, response plan, qualify the breaches, etc.).

Good practices to be followed if the measure is used to address risks:

- Define the roles and responsibilities of the stakeholders, as well as procedures for providing feedback and responses in the event of a personal data breach.
  - ♦ *Recommendations: formally document the responsibilities of the "data protection" correspondent (DPO or equivalent), interactions with the CNIL, the data subjects and establish a crisis response unit in the event of a damaging event.*
- Establish a directory of individuals responsible for managing personal data breaches.
- Develop a response plan in the event of a personal data breach for each high risk, update it and test it periodically.
  - ♦ *Recommendations: test the plan at least once every two years.*
- Categorize the personal data breaches based on their impact on data subjects' freedoms and privacy.
  - ♦ *Recommendations: an event is a personal data breach without impacts; an incident corresponds to a personal data breach with isolated impacts; a damaging event is a personal data breach with significant, immediate impacts for one or more subjects; a crisis is a personal data breach with significant, more long-term consequences for one or more subjects.*
- Handle the incidents based on their categorization (event, incident, damaging event or crisis.). ♦ *Recommendations*
  - ◊ *if the breach involves an event, record it and notify the "data protection" correspondent (DPO or equivalent);*
  - ◊ *if the breach involves an incident, resolve it and, where applicable, notify the data subjects concerned by the breach (notification of a data breach is not necessary if the latter does not pose a high risk to the rights and freedoms of the data subjects, if the data controller has demonstrated, to the satisfaction of the competent authority, that it has implemented the appropriate technological protection measures and that those measures were applied to the data concerned by the breach. Such technological measures shall render the data unintelligible to any person who is not authorized to access the data);*
  - ◊ *if it involves a damaging event, also initiate an in-depth analysis;*
  - ◊ *if it involves a crisis, also initiate an established management plan.*

- Keep up-to-date documentation on data breaches as provided for in Article 33-5 of the General Data Protection Regulation (GDPR).
    - ♦ *Recommendations: record the context of the data breaches, the category of data subjects and records concerned, the volume of data subjects and records concerned, the breach effects and the measures taken to address them.*
- Analyze the possibility of improving the security measures based on the personal data breaches that have occurred.

Notes

- The "Telecoms Package" adopted by the European Parliament in 2009 and transposed into French law in 2011 creates an obligation to notify the CNIL of certain personal data breaches. This obligation has been rolled out to involve all data controllers, not only "providers of publicly available electronic communications services" by the GDPR, due to come into force in May 2018. These texts define the form of such notifications:
    - ♦ in the event the data breach poses a high risk to the rights and freedoms of data subjects, notification of the latter shall describe, at a minimum, the nature of the personal data breach and the contacts from whom additional information may be obtained and shall recommend measures to mitigate possible negative impacts of the personal data breach;
    - ♦ notification of the national authority with jurisdiction (in France, the CNIL) shall also describe the impacts of the personal data breach and the measures proposed or taken by the provider to remedy it. Under the GDPR, said notification is necessary the moment the breach results in a risk for the rights and freedoms of data subjects.
    - ♦ This obligation is not exclusive and does not cancel the notification obligations set out in other national or European texts.
- It is important to be able to gather, preserve and present proof when legal action follows an incident.

Tools/To find out more

- See the CLUSIF-Victim procedure.
- See the CERTA-Intrusion briefing note.
- See Directive 2009/136/EC.
- See Articles 33 & 24 of the GDPR.

18 Staff management

Aims: to reduce the possibility of the characteristics of certain persons (employees, individuals who are not part of an organization but are under its responsibility, etc.) being used to adversely affect personal data (adequate skills and resources, awareness-raising, etc.).

Good practices to be followed if the measure is used to address risks

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

Tools/To find out more

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

19 Management of workstations

19.1 General measures

Aims: to reduce the possibility of the characteristics of software (operating systems, business applications, database management systems, configurations, etc.) being used to adversely affect personal data (updates, physical protection and access, work on a backed-up network space, integrity checkers, logging, etc.).

Good practices to be followed if the measure is used to address risks

- Ensure that the IT department provides users with workstations that are kept secure and in working order.
- Small workstations, especially laptops, can be easily stolen. They must therefore be equipped with anti-theft cables whenever their users are not nearby and the premises are not protected by physical security measures.
- Retrieve data, except for data defined as private or personal, from workstations before they are assigned to other persons.
- Erase data from workstations before assigning them to other persons or if such workstations are shared.
- Delete temporary data each time a person logs onto a shared workstation.
- If a workstation becomes compromised, inspect the system for all signs of intrusion in order to determine whether other information has been compromised by the attacker.
- Maintain systems and applications up-to-date (versions, security patches, etc.) or, where this is not possible (e.g. applications available only on a system that is no longer supported by the software company), isolate the machine and closely monitor the logs.
    - ♦ *Recommendations: use versions maintained by the manufacturer or another service, update software without delay by programming a weekly automatic check, test the updates before deploying them across the system, ensure that the updates can be reversed in the event their application fails and regularly check that the software licenses are valid for example.*
- Document configurations and update them whenever major changes are made.

♦ *Recommendations: procedures for strengthening IT resources are described; the links required to perform security updates during installation are identified, etc.*

- Reduce the possibilities of misuse.
    - ♦ *Recommendations: manage individual access rights according to the principle of least privilege (avoid, in particular, authorizing the use of advanced functionalities where such authorization is not necessary); assign public or private IP addresses where they are actually needed; disable or delete services that are not absolutely necessary; disable or delete unnecessary accounts (guest accounts, default vendor support accounts, etc.); prohibit logical access to remote diagnostic and configuration ports,*

disable autorun when a removable device is inserted, boot only from the local drive or the local memory, etc.

- Protect access points.
  - ♦ *Recommendations: protect the low-level system configuration (e.g. BIOS) with a password, change the default passwords, block access to the system with a password-protected screensaver that activates after a period of inactivity (5 minutes for maintenance work, no more than 15 minutes for routine use), display last login dates and times when logging into accounts, etc.*
- Enable protection measures afforded by the system and the applications.
  - ♦ *Recommendations: enable login passwords, the firewall, automatic updates, malware protection, etc., wherever this is allowed by the operating system; enable access controls on applications that feature them, etc.*
- Prohibit local sharing of directories or data on workstations.
- Store user data on a backed-up network space, not on workstations.
- If data must be stored on a local workstation, provide users with means of synchronization or backup and inform them how to use these means.
  - ♦ *Recommendations: individual spaces on file servers with a detailed filing plan; automatic scripts for copying local folders; automatic synchronization tools managed by the IT department, etc.*
- Secure the configuration of Web browsers.
  - ♦ *Recommendations: this configuration must include the protection of personal information stored by browsers (forms, passwords, certificates, etc.), the use of a master password in Mozilla Firefox, the impossibility of storing passwords if there are high risks, etc.*
- Deploy a secure browser on all servers that are to be used to access the Internet or an intranet.
- Limit the number of plugins, remove any that are not used, regularly update those that are left installed.
- Prohibit the use of downloaded applications that are not from safe sources.
- Search for exploitable vulnerabilities.
  - ♦ *Recommendations: actively monitor for vulnerabilities found in software used to process data; use vulnerability detection tools (vulnerability scanning software such as Nmap and Nikto) and even intrusion detection and prevention systems (Host Intrusion Prevention); make sure that top vulnerabilities are covered, etc.*
- Check system integrity using integrity checkers (which check the integrity of selected files).
  - ♦ *Recommendations: continuously monitor changes made to certain files or directories (use software such as Tripwire); check the registry and processes launched by the system (use software such as Spybot); identify the presence of rootkits (use software such as Rootkit Revealer), etc.*

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

Tools/To find out more

- Depending on the type of application, it may be necessary to ensure the integrity, availability and, where necessary, the confidentiality of software and of source codes of internally developed applications, especially if they are rare, innovative or of high market value, by appending signatures to the executable code to guarantee that it has not been altered. In that regard, signature verification during execution (not just prior to execution) makes compromising a program harder.

19.2 Specific measures for mobile devices

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

Good practices to be followed if the measure is used to address risks

- Encrypt personal data stored on mobile devices.
    - ♦ *Recommendations: physically encrypt the entire hard disk, logically encrypt the entire hard disk via the operating system, encrypt files individually, create encrypted containers, etc.*
- Limit the amount of personal data stored on mobile devices to the strict minimum, and prohibit such storage during travel abroad if needs be.
- Ensure the availability of personal data stored on mobile devices.
    - ♦ *Recommendations: copy personal data to another computer or another server as soon as possible, etc.*

- Erase personal data from mobile devices as soon as such data is entered in the organization's information system.
- Place privacy filters on mobile devices whenever they are used outside the organization.

Notes

- More and more laptops are equipped with fingerprint readers. The use of such readers is subject to authorization from the CNIL.
- Disk encryption should not be disabled. A copy of the keys should be retained when encryption is available.

Tools/To find out more

- See the ANSSI-Voyagers guide for travel abroad.

19.3 Specific measures for cellphones/smartphones

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

Good practices to be followed if the measure is used to address risks

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

immediately install operating system security updates, authenticate devices with digital certificates (where possible), etc.

- Secure phones at the end of their life cycle.
  - ♦ Recommendations: before disposing of a phone or recycling it, erase all of its data and settings and implement a detailed phone dismantlement procedure that includes wiping the phone's memory.

Tools/To find out more

- See the CNIL-Smartphones article.
- See the CLUSIF-Voice guide.
- See the ENISA-Smartphone report.
- More rigorous measures may be taken where risks are considered to be too high: block attachments; trace and analyze traffic with a sensor; verify the effectiveness of encryption; do not store sensitive data locally and do not allow online access to sensitive data using a smartphone with a non-cached application; do not send sensitive files to smartphones by email if there are high risks; use end-to-end SMS encryption software; draw up a whitelist of authorized applications; regularly reinstall a specially made and tested image of the drive, etc.).

20 Project management

Aims: to integrate the protection of personal data in all new processing operations (trusted names, guidelines, CNIL risk management, CNIL formalities).

20.1 General measures

Good practices to be followed if the measure is used to address risks

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

Tools/To find out more

- See "Adapting ISS to the issues at stake", "Using products and providers awarded with security certification", and "Efforts commensurate with ISS stakes" in the General Security Framework (RGS).
- See the rules and recommendations on "Acknowledging registration and acknowledging receipt" in the RGS and the associated appendices
- See the catalogues of products recognized by ANSSI.
- See the ANSSI SSI Maturity and ANSSI GISSIP guides.

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

Good practices to be followed if the measure is used to address risks

- Make sure that developers and maintainers have sufficient resources to perform their tasks.

- ♦ Recommendations: check for clear specifications, suitable documentation, sufficient skills, etc.

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

Tools/To find out more

- See the General inoperability framework.

21 Risk management

Aims: to control the risks that processing operations performed by the organization pose on the rights and freedoms of data subjects (listing of personal data processing, data, supporting assets, risk assessment and determine existing or planned measures, etc.).

Good practices to be followed if the measure is used to address risks

- List the personal data processing operations, whether automated or otherwise, the data processed (e.g. client files, contracts) and the supporting assets on which they rely:
  - ♦ hardware (e.g.: human resource management server, laptop, CD-ROM);
  - ♦ software (e.g.: operating system, business software);
  - ♦ communications channels (e.g. fiber optics, Wi-Fi, Internet);
  - ♦ paper documents (e.g.: printed document, photocopy).
- Assess the way in which the fundamental principles (information, consent, right of access, etc.) are respected.
- Assess the risks of each processing.
  - ♦ Identify the potential impacts (what might the consequences be on the rights and freedoms of the data subjects?) for the three risks below:
    - ◊ Illegitimate access to personal data: (e.g.: identity thefts following the disclosure of all of the payslips of a company's workforce);
    - ◊ unwanted change of data (e.g.: wrongful accusation of a person following a change in access logs);
    - ◊ disappearance of data (e.g.: non detection of a medicinal interaction because of the impossibility of accessing the patient's electronic record).
  - ♦ Identify the risk sources (who or what could be behind each risk?), with account taken of:
    - ◊ the internal and external human sources, whether accidental or intentional (e.g.: IT administrator, user, external hacker, competitor);
    - ◊ internal or external non-human sources (e.g. water, hazardous materials, non-targeted computer virus).
  - ♦ Identify the threats that could materialize (what could enable each risk to occur?). Such threats materialize via data supporting assets (hardware, software, communications channels, paper documents, etc.), which may be:
    - ◊ used inappropriately (e.g.: abuse of rights, handling error);
    - ◊ altered (e.g.: software or hardware tracking, keylogger, unintentional installation of malware);
    - ◊ lost (e.g.: theft of a laptop, loss of a USB flash drive);

- ◊ observed (e.g. watching a person's screen without their knowledge while on the train; taking a photo of a screen; geolocation of hardware);
- ◊ damaged (e.g.: vandalism, deterioration due to natural wear);
- ◊ overloaded (e.g.: full storage unit, denial of service attack).

♦ Determine the existing or planned measures (technical and organizational) for addressing each risk (e.g. access control, backups, traceability, security of premises, encryption, anonymization).

♦ Estimate the severity and likelihood of the three risks, in light of the previous information and given the existing or controlled measures (example of useable scale for this estimation: negligible, moderate, significant, maximum).

♦ *Recommendations: the table below can be used to document this estimation:*

Risks	Impacts on data subjects	Main risk sources	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access to personal data						
Unwanted change of data						
Disappearance of data						

- Implement and check the planned measures. Where the existing and planned measures are considered appropriate for guaranteeing the right level of security in light of the risks, their application and monitoring must be ensured.
- Make sure a security audit is carried out periodically – annually where possible. Each audit must be accompanied by an action plan, the implementation of which should be monitored at the highest level.
- Update the map periodically and at each major change.

♦ *Recommendations: each time a new processing operation is created and at least once a year by a dedicated committee.*

Tools/ To find out more

- Regulation (EU) 2016/679 of April 27, 2016 introduces the notion of "data protection impact assessment" and stipulates that this shall contain at least "*a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality, an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to*

ensure the protection of personal data and to demonstrate compliance with this Regulation" (see Article 35.7). The estimation of the risks discussed in this paper can be used to inform the impact assessment.

- Use of a proper method provides practical tools and improves the exhaustiveness and depth of the risk analysis. To that end, the CNIL's PIA (*Privacy Impact Assessment*) guides can be used to carry out a data protection impact assessment.
- The information security risks can be studied at the same time as the privacy risks. Since the two study approaches are compatible, it is not difficult to combine them.
- By studying the risks it is possible to determine the technical and organizational measures that need setting up. A budget must therefore be drawn up to implement them.
- See the General Security Framework (RGS).
- See the EBIOS method.

22 Information for the data subjects (fair and transparent processing)

22.1 General measures

Aims: to comply with Article 32 of the DP-Act and Articles 12, 13 and 14 of the General Data Protection Regulation (GDPR); to guarantee that the data subjects are informed and therefore prevent data from being collected without their knowledge; to confirm that the processing is not subject to an exception or specific conditions mentioned in Article 32 of the DP-Act (electronic communications networks user, statistics, anonymization, national security, defense, public safety, enforcement of criminal sentences, security measures, prevention, research, reporting or prosecution of criminal offences).

Good practices

- Determine and justify the practical means that will be implemented to inform the data subjects, or justify when they are impossible to implement:
  - ♦ presentation of the terms & conditions for use/confidentiality;
  - ♦ possibility of accessing the terms & conditions for use/confidentiality;
  - ♦ legible and easy-to-understand terms;
  - ♦ existence of clauses specific to the device;
  - ♦ detailed presentation of the data processing purposes (specified objectives, data matching where applicable, etc.);
  - ♦ detailed presentation of the personal data collected;
  - ♦ presentation of any access to the identifiers of the device, by specifying whether these identifiers are communicated to third parties;
  - ♦ presentation of the data subject's rights (consent withdrawal, data erasure, etc.);
  - ♦ information on the secure data storage method, particularly in the event of sourcing;
  - ♦ arrangements for contacting the company (identity and contact details) about confidentiality issues;
  - ♦ where applicable, information for the user on any change concerning the data collected, the purposes and confidentiality clauses;
  - ♦ Regarding transmission of data to third parties:
    - ◊ detailed presentation of the purposes of transmission to third parties;
    - ◊ detailed presentation of the personal data transmitted;
    - ◊ indication of the identity of third-party undertakings.
- Ensure that the notification is complete, clear and appropriate to the target audience based on the nature of the personal data and the practical means chosen.

- ♦ *Recommendations: present the information in clear language that can be understood by a person who is not familiar with information technologies or the Internet.*

- Ensure that the notification is provided by the time the data are collected.
- Ensure that the data cannot be collected without providing this information.
  - ♦ *Recommendations: determine alternative solutions in the event that the practical means are no longer operational.*
- If possible, provide a means by which to show that notification was provided.
  - ♦ *Recommendations: post this information on a board that all employees are bound to have seen or require that a notice or document be signed or initialled, etc.*

Notes

- The notification must be delivered individually (for example, in a verbal exchange or a pop-up window), but may be done collectively (by note or poster in a premises) if the data controller is sure that all data subjects will have easy access to this method.
- The notification must include the identity of the data controller, the purpose of the processing, whether the information collected is required or optional, the consequences for failing to respond, the recipients of the information, the subject's rights, the person responsible for enforcing the rights and the projected transfers of the data.
- NB: in the event that data are transmitted to third-party bodies linked to the data controller (subsidiaries, members, intra-group, partners, etc.), it is necessary to supply the list of recipients (in a dedicated information section), clarifying the data categories transmitted and the transfer purpose, and providing a hyperlink to the data protection policy of the respective recipients. An internal process must also be planned so as to be able to update this list in the event of changes.

Tools/To find out more

- See Article 32 of the DP-Act and Articles 12, 13 & 14 of the GDPR for the content of the notification, exceptions and specific conditions.
- See the legal notice templates on the CNIL website (https://www.cnil.fr/fr/modeles/mention).
-

22.2 Specific measures for employees of an organization

Good practices

- Obtain the prior opinion of the staff representative organizations in the cases set forth in the French Labor Code.
- Use the method that is most appropriate to the organization.

- ♦ *Recommendations: posters, internal memos, email, specific forms, employment contract, internal regulations or the IT charter.*

22.3 Specific measures for collecting personal data via a website

Good practices

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

22.4 Specific measures for collecting data via a connected object or mobile app

Good practices

- Provide direct or easily accessible information for users.
  - ♦ *Recommendations: display a message when the device or mobile app is first activated, and then make this information accessible via a specific menu; place an information "QR Code" on the device if it does not have a screen.*
- Inform the user if the app is likely to access the device's identifiers, by specifying whether these identifiers are communicated to third parties.
- Inform the user if the app is likely to run in the background.
- Present the protections for accessing the device to the user.

22.5 Specific measures for collecting personal data by telephone

Good practices

- Issue an automatic message before the conversation begins with information on subjects' rights, the reason for recording the conversation (for training purposes or to monitor service quality), if necessary, and an opportunity to object to recording (on legitimate grounds).
- Set up means for authenticating the caller (e.g.: via information that is known only to the organization and data subject).

22.6 Specific measures for collecting data via a form

Good practices

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

22.7 Specific measures for using targeted advertising techniques

Good practices

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

Tools/To find out more

- See the opinion G29-Advertising.

22.8 Specific measures for updating existing processing

Good practices

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

23 Clamping down on malware

Aims: to protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of personal data (antivirus, firewall, proxy, anti-spyware, reporting of security events, etc.).

Good practices to be followed if the measure is used to address risks

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

Tools/To find out more

- See the briefing note reminder on Trojan horses and viruses, CERTA.
- See the briefing note reminder on inbox viruses, CERTA.

24 Maintenance

24.1 General measures

Aims: to limit the likelihood of threats associated with maintenance operations on hardware and software (procurement contract, remote maintenance, user's agreement, erasure of data, etc.).

Good practices to be followed if the measure is used to address risks

- Establish a procurement contract to govern maintenance operations when they are carried out by service providers (see the page Relations with third parties).
- Record all maintenance operations in a logbook.
- Govern remote maintenance operations.
  - ♦ *Recommendations: systematically use encrypted communications channels, use robust authentication keys or passwords, log accesses (see the page Traceability (logging)).*
- Encrypt or erase data contained on hardware (desktop computers or laptops, servers, etc.) that are sent for external maintenance. If this is not possible, remove the equipment storage devices before dispatch to maintenance or manage maintenance internally.

24.2 Specific measures for workstations (desktop computers and laptops, smartphones, tablets)

Good practices to be followed if the measure is used to address risks

- During maintenance operations that require remote access to a workstation, only perform the operation after obtaining the user's agreement, and indicate to the latter on the screen if the access is effective.
- When a maintenance operation requires physical intervention on a workstation containing sensitive data in the meaning of Article 8 of the DP-Act and data coming under Article 9 of the same Act, delete the data during the maintenance.
- Configure telephones before delivering them to users.
  - ♦ *Recommendations: telephones must automatically lock after a period of inactivity (1 to 5 minutes), the memory card (microSD) on which email is stored must be encrypted, the remote lock must be activated so that the contents may be erased in the event of loss or theft, the installation of new applications is restricted (where possible) and all of these measures must be managed by a fleet management system making it possible to enforce application of these rules.*
- Inform users, such as in a memo provided at delivery, about how to use their phone, the applications installed on it *(e.g. Business Mail, Exchange,* etc.), the services provided, and the security rules to be followed.

- ♦ *Recommendations: users must not open email of unknown origin, they must not store sensitive files (apart from when reading email), they must regularly erase their telephone's cache and cookies, they must immediately notify the IT department in the event of loss, theft or abnormal functioning of the telephone, they must not install any software on their phone unless they are expecting to receive such content and it has been sent by a trusted source (check the reputation of the source before installing or using applications or services).*

- Secure phones at the end of their life cycle.
  - ♦ *Recommendations: before disposing of a workstation or recycling it, erase all of its data and settings and implement a detailed dismantlement procedure that includes wiping the memory, etc.*

24.3 Specific measures for storage devices

Good practices to be followed if the measure is used to address risks

- Erase all contents securely or physically destroy storage devices that are discarded.
  - ♦ *Recommendation: wipe magnetic storage devices (hard disks, tapes, etc.) using secure erasing software (particularly see the list of erasing software certified by ANSSI) or a degausser, or call on a service provider specializing in the destruction of storage devices.*
- During maintenance operations that require remote access to a workstation, only perform the operation after obtaining the user's agreement.

24.4 Specific measures for multifunction printers and copiers

Good practices to be followed if the measure is used to address risks

- If maintenance is performed by a third party, set up measures to block access to personal data.
  - ♦ *Recommendations: data must be either securely encrypted or erased before hardware is sent out for maintenance; have the maintenance company sign a confidentiality agreement or have the repairs performed on-site in the presence of a member of the IT department where data are sensitive and cannot be completely encrypted or erased (hard disk failure, malfunction, etc.); prohibit hardware containing sensitive data from being sent out for maintenance, etc.*
- If a locally networked multifunction printer or copier is maintained remotely by a third party, take specific measures to protect access to this equipment.
  - ♦ *Recommendations: have the external third party sign a confidentiality agreement, use individual robust passwords that are changed on a regular basis, enable dial-in access for remote maintenance purposes only when requested, dial-in access should be disabled by default, keep a remote*

maintenance access log, prohibit the possibility of using remote maintenance to bounce to the rest of the LAN and more generally the Internet, etc.

- Block access to personal data stored on discarded multifunction printers or copiers.
  - ♦ *Recommendations: store equipment on-site in a secure room until it is taken away, use a secure erasing tool to wipe data from hard disks or built-in memory, if wiping is not possible (due to failure, malfunction, etc.), physically destroy equipment, if equipment disposal is contracted out, have the disposal company sign a confidentiality agreement, issue an equipment destruction report and retain it for 10 years.*

26 Data minimization: adequate, relevant and limited

26.1 Collection minimization

Aims: to comply with Article 6 of the DP-Act and Article 5.1(c) of the General Data Protection Regulation (GDPR); to reduce the severity of risks by limiting the amount of personal data to what is strictly necessary to achieve a defined purpose; to avoid collecting unnecessary data, using data with no bearing on the end purpose and excessive impacts for data subjects.

Good practices

- Justify the collection of each piece of data.
- Clearly distinguish between anonymous and pseudonymous data.
- Avoid free-form text fields (of the "comments" space type), because of the risk that users note down information that does not comply with the minimization principles there. Preference should therefore be given to scroll-down list type fields. If free-form text fields cannot be avoided, users' awareness must be raised in how to use such fields, with regard to the standard terms & conditions for service and the law (no offensive words, no undeclared sensitive data, etc.).
- Confirm that the personal data are adequate, relevant and not excessive with regard to the intended purpose; otherwise, do not collect the data.
  - ♦ *Recommendations: define the purpose of the processing, identify the personal data necessary to achieve that purpose, demonstrate why each category of personal data is vital and, last, rule out any personal data which do not prevent the purpose from being achieved; if necessary, review the purpose if the data are necessary for something other than the initial intended purpose.*
- Confirm that the personal data do not reveal (directly or indirectly) racial or ethnic origin, political, philosophical or religious views, trade union membership, health information or information on an individual's sex life and do not collect them if they do, except under exceptional circumstances (for example, with consent, in the public interest or pursuant to Article 8 of the DP-Act and Article 9 of the GDPR).
- Confirm that the personal data do not relate to offences, criminal convictions or security measures and do not collect them if they do, except under exceptional

circumstances (for example, in dealing with the courts or court officers pursuant to Article 9 of the DP-Act and Article 10 of the GDPR).

- Prevent the collection of additional personal data.
  - ♦ *Recommendations: only fields that relate to the personal data defined are to be created and may be entered in a database and no additional field may be added (do not include a "free-form text field" but scroll-down lists; if free-form text fields cannot be avoided, warn users), check at regular intervals that no additional data have been collected in light of what was initially intended.*

Notes

- Some categories of data are subject to specific restrictions (in particular, so-called "sensitive data" and data "regarding offences, criminal convictions and security measures" which only certain categories of legal entities may process, pursuant to Articles 8 and 9 of the DP-Act and Articles 9 and 10 of the GDPR).
- Due to the sensitive nature of data concerning a minor and bearing in mind the principle of fair collection as regards a vulnerable user, the collection of data concerning a child, his/her parents or family must be particularly limited and justified.

26.2 Minimization of data themselves

Aims to comply with Article 6 of the DP-Act and Article 5.1(c) of the GDPR; to reduce the severity of risks by minimizing the data themselves, by taking measures aimed at reducing their sensitivity.

Good practices

- Filter and remove unnecessary data.
  - ♦ *Recommendations: When data are being imported, different types of metadata (such as EXIF data with an image file attached) can unintentionally be collected. Such metadata must be identified and eliminated if they are unnecessary for the purposes specified.*
- Reduce sensitivity via conversion.
  - ♦ *Recommendations: once sensitive data have been received, as part of a series of general information or transmitted for statistical purposes only, these can be converted into a less sensitive form or pseudonymized.*
    For example:
    - ◊ *if the system collects the IP address to determine the user's location for a statistical purpose, the IP address can be deleted once the city or district has been deduced;*

- ◊ *if the system receives video data from surveillance cameras, it can recognize people who are standing or moving in the scene and blur them;*
- ◊ *if the system is a smart meter, it can aggregate the use of energy over a certain period, without recording it in real time.*

- Reduce the identifying characteristics of data (See the section Anonymization).
  - ♦ *Recommendations: the system can ensure that:*
    - ◊ *1) the user can use a resource or service without the risk of disclosing his/her identity (anonymous data);*
    - ◊ *2) the user can use a resource or service without the risk of disclosing his/her identity, but remain identifiable and responsible for this use (pseudonymous data);*
    - ◊ *3) the user can make multiple uses of resources or services without the risk of these different uses being linked together (data cannot be correlated);*
    - ◊ *4) the user can use a resource or service without the risk of others, third parties in particular, being able to observe that the resource or service is being used (non-observability).*
  - ♦ *The choice of a method from the list above must be made on the basis of the threats identified. For some types of threat to privacy, pseudonymization will be more appropriate than anonymization (for example, if there is a traceability need). In addition, some threats to privacy will be addressed using a combination of methods.*
- Reduce data accumulation.
  - ♦ *Recommendations: the system can be organized into independent parts with separate access control functions. The data can also be divided between these independent sub-systems and controlled by each sub-system using different access control mechanisms. If a sub-system is compromised, the impacts on all of the data can thus be reduced.*
- Restrict access to data.
  - ♦ *Recommendations: the system can limit data access according to the "need to know" principle. The system can separate the sensitive data and apply specific access control policies. The system can also encrypt sensitive data to protect their confidentiality during transmission and storage. Access to temporary cookies which are produced during the data processing must also be protected.*
- Restrict the transmission of electronic documents containing personal data to the individuals who need them in connection with their work.
- Securely delete personal data that are no longer necessary or that a subject requests be deleted from the system in operation or from backups where applicable (also see the page Storage durations: limited).
  - ♦ *Recommendations: use a secure erasing tool for electronic documents and a degaussing device for storage units that use magnetic technologies.*

Tools/To find out more

- See the list of products that have received first-level security certification (FLSC) of the French Network and Information Security Agency (ANSSI) on http://www.ssi.gouv.fr/).
- See the guide on ANSSI-Erasure and certified secure erasing software.

27 Organization

Aims: to obtain an organization able to manage and control the protection of personal data held within it (appoint a DPO, set up a monitoring committee, etc.).

Good practices to be followed if the measure is used to address risks

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

Notes

- Appointing a DPO provides a degree of legal certainty (as the DPO ensures compliance with the DP-Act and GDPR), helps simplify administrative procedures (exemption from the requirement of prior notification of ordinary and routine processing operations), offers personalized access to the CNIL's services (extranet, training, personalized follow-up, etc.), demonstrates a commitment to ethical and socially responsible management, and provides a means of capitalizing on informational assets (possibility of assigning, transferring or renting files held by the organization in accordance with the DP-Act).

28 Policy (management of rules)

Aims: to obtain a documentary base setting out data protection objectives and rules (action plan, regular review of the data protection policy, etc.).

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- See "Developing an ISS policy" in the General Security Framework (RGS).
- See the ANSSI-PSSI guide.

29 Protection against non-human risk sources

Aims: to reduce or avoid risks associated with non-human sources (including climate events, fire, water damage, internal or external accidents and animals) that could affect the security of the personal data (prevention measures, detection, protection, etc.)

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

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

30 Data quality: accurate and kept up-to-date

Aims: to comply with Article 6 of the DP-Act and Article 5.1(d) of the General Data Protection Regulation (GDPR); maintain the quality of data to avoid computing on the basis of incorrect or obsolete data.

Good practices

- Regular checks of the accuracy of the user's personal data.
- Ask the user to check and, where necessary, update his or her data at regular intervals.
- Ensure the traceability of any data changes.

Notes

- The quality requirement also concerns the link between the data identifying the people and the data concerning them.

31 Obtaining consent

31.1 General measures

Aims: to comply with Article 7 of the DP-Act and Articles 7 and 8 of the General Data Protection Regulation (GDPR); allow freely given, specific and informed choice; determine whether the processing relies on a legal basis other than consent, as set forth in Article 7 of the DP-Act and Article 6 of the GDPR (legal obligation, protection of vital interests, public service mission, contract or measures undertaken with the data subject, legitimate interest).

Good practices

- Determine and justify the practical means to be implemented to obtain the consent of the data subjects or justify when they are impossible to implement:
  - ♦ express consent upon registration;
  - ♦ consent segmented per data category or processing type;
  - ♦ express consent prior to sharing data with other users;
  - ♦ consent presented in an intelligible and easily accessible form, using clear and plain language adapted to the target user (particularly for children);
  - ♦ obtaining parents' consent for minors under 13 years of age;
  - ♦ for a new user, consent must once again be obtained;
  - ♦ after a long period without use, the user must be asked to confirm his/her consent;
  - ♦ where the user has consented to the processing of special data (e.g. his/her location), the interface clearly indicates that said processing takes place (icon, light);
  - ♦ if the user changes contract, the settings associated with his/her consent are maintained.
- Ensure that consent is obtained before any processing begins.
  - ♦ *Recommendations: analyze the cases in which the practical means chosen are no longer operational and identify backup solutions, if necessary.*
- Ensure that consent is obtained freely.
  - ♦ *Recommendations: confirm that an alternative exists that is not overly restrictive (it must provide a choice) and that no hierarchical relationship exists (for example, between an employee and his/her employer).*
- Ensure that the consent is obtained in an informed, transparent manner in terms of the purposes of the processing.
- Ensure that consent is obtained for a specific purpose.
- When procurement is involved, set out each party's obligations in an explicit written agreement accepted by both parties.
- Obtain the parents' consent for minors under 13 years of age.

Notes

- The CNIL considers that an employee cannot consent freely to processing set up by his/her employer given their hierarchical relationship.
- The practical means for obtaining consent include actions that an individual must perform (for example, entering a PIN - Personal Identification Number, placing a cellphone close to a smart poster when advertisements are sent from a smart poster to a telephone via Bluetooth or requiring that a NFC - Near Field Communication peripheral be placed close to a reader).
- For any direct provision of information society services to minors, the burden of proof of consent lies with the data controller (or processor), who must endeavor to check that the holder of parental responsibility has indeed consented (reasonably, in view of the available technological means).

Tools/ To find out more

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

31.2 Specific measures for data under Article 8 of the DP-Act

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

Good practices

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

31.3 Specific measures for collecting personal data via a website

Good practices

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

31.4 Specific measures for collecting personal data via cookies

Good practices

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

Notes

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

Tools/ To find out more

- See the factsheets https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite and https://www.cnil.fr/fr/recommandation-sur-les-cookies-quelles-obligations-pour-les-responsable on the CNIL website.

31.5 Specific measures for collecting data via a connected object or mobile app

Good practices

- Obtain the user's consent when the mobile app or device is first activated.
  - ♦ *Recommendations: obtain consent again when a new user is accessing the mobile app or device; after a long period without use, ask the user to confirm his/her consent; maintain the consent settings if the device is changed or app reinstalled.*
- Offer consent segmented per data category or processing type, particularly by distinguishing data sharing with other users or third-party companies.
  - ♦ *Recommendations: where the user has consented to the processing of special data (e.g. his/her location), the interface clearly indicates that said*

processing takes place (icon, light); allow the user to access his/her consent settings at any time.

31.6 Specific measures for geolocation via a smartphone

Good practices

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

31.7 Specific measures for using targeted advertising techniques

Good practices

• Provide users with simple, no-cost methods to accept or refuse advertising based on their navigation behavior and to choose the targeted advertising they would like to receive based on their interests.

♦ *Recommendations: provide Internet users a platform from which to accept or refuse, completely or in part, the display of targeted behavioral advertising; explain how to delete cookies and browser histories, authorize or prohibit the storage of cookies; and allow cookies to be created and stored showing that the user has chosen not to receive behavioral advertising from third parties.*

31.8 Specific measures for research using identifiable biological samples (i.e. DNA)

Good practices

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

32 Relations with third parties

32.1 General measures

Aims: to reduce the risk that legitimate access to personal data by third parties may pose to the data subjects' freedoms and privacy (identification of third parties, procurement contract, agreement, binding corporate rules/BCR, etc.).

Good practices to be followed if the measure is used to address risks

- Identify all third parties who have or could have legitimate access to personal data.
  - ♦ *Recommendations: certain categories of employees, seconded employees (service providers), IT maintenance, business partners and authorized third parties.*
- Determine their role in the processing (including IT administrators, processors, recipients, persons responsible for processing data and authorized third parties) based on the actions they will perform.
  - ♦ *Recommendations: if using a cloud computing service provider, the latter is generally a processor although, in some cases, may be considered to be the data controller.*
- Determine the respective responsibilities based on the risks connected to the personal data.
- Determine the appropriate form for establishing rights and obligations based on the third parties' legal structure and their geographic location.
  - ♦ *Recommendations: a procurement contract, an agreement, an order or binding corporate rules (BCR).*
- Formally document the rules that persons must comply with throughout the life cycle of the relationship related to the processing or the personal data, based on the person's category and the actions that he/she will perform.

Tools/ To find out more

- See the briefing notes CNIL Transfer outside the EU and CNIL Outsourcing outside the EU for transfers of data outside the European Union.

32.2 Specific measures for third-party service providers working on the organization's premises

Good practices to be followed if the measure is used to address risks:

- Apply to said service providers the same measures as for the organization's employees: training in data protection issues, requirement to comply with the rules for using the organization's IT resources, appended to the rules of procedure.

- Provide said service providers with a workstation inside the organization or check that use of the workstation supplied by their employer is compatible with the organization's security objectives.
- Make sure said service providers are properly bound with their employer by a confidentiality clause applicable to their employer's client organizations.
- Manage clearance authorizations for such service providers specifically by granting time-bound authorizations that automatically end on the provisional end date for their assignment.
-

32.3 Specific measures for third-party recipients

Good practices to be followed if the measure is used to address risks

- Govern the transmission of data to said third-parties via a contract setting out:
  - ♦ Which data are transmitted.
  - ♦ The purpose(s) for which the data subjects have consented to their data being transmitted to the third party (subscription to a newsletter, marketing, etc.).
  - ♦ The conditions under which the data subjects may exercise their rights.
  - ♦ The technical measures taken to ensure data security when they are being transmitted to the third party.
- Require the third party to publish a privacy protection policy covering the processing making use of the data transmitted and outlining the security objectives pursuant to the IT system security policy.
- If data are transmitted via the Internet, always encrypt the data flows.
- Systematically inform the third party when the data subjects exercise their right to rectification.

32.4 Specific measures for authorized third parties

Good practices to be followed if the measure is used to address risks

- Only reply to requests that are officially sent (by mail or fax) and reply using the same communications channel. Do not take account of requests sent by email and do not reply using this communications channel.
- Check the legal basis of each request for communication.
- Authenticate the parties submitting the requests and only reply to them.
- Reply strictly to the request by only supplying the data asked for in the request.

33 Backups

Aims: to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality (regular backups, encryption of the data transmission channel, integrity test, etc.).

Good practices to be followed if the measure is used to address risks

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

Notes

- Transfers of personal data (and, thus, of backups) to countries outside the European Union are prohibited unless:
  - ♦ they involve a transfer to a country that the European Commission recognizes as “adequate”;
  - ♦ the issuer and recipient of the data have signed model contract clauses approved by the European Commission;
  - ♦ binding corporate rules (BCR) have been adopted (within a group);
  - ♦ in the case of a transfer to the U.S., the recipient company has opted into the Privacy Shield program;
  - ♦ one of the exceptions set forth in Article 69 of the DP-Act is invoked.
- The CNIL website includes a world map indicating the formalities to be followed for each country. In all cases, the data controller remains responsible for the security of the backed-up personal data.
- The setup of a backup procedure and plan must make it possible to ensure the integrity and sustainability of the personal data, without endangering their confidentiality for all that. The backup plan must demonstrate the expected general objectives of the backups in terms of data protection and determine the necessary organizational measures for achieving them. The backup procedure shall determine the operational and technical means that must be taken to honor the backup plan.

34 Procurement: identified and governed by a contract

34.1 General measures

Aims: to comply with Article 28 of the General Data Protection Regulation (GDPR); regulate the procurement.

Good practices

• A procurement contract must be signed with each processor, setting out all of the points stipulated in Art. 28 of the GDPR:

- ♦ procurement scope and duration,
- ♦ procurement purpose,
- ♦ documented processing instructions,
- ♦ prior authorization in the event another processor is used,
- ♦ provision of any documentation demonstrating compliance with the GDPR,
- ♦ immediate notification of any data breach,
- ♦ etc.

34.2 Specific measures for processors (host, maintenance company, administrator, specialist service providers, etc.) excluding providers of cloud computing services

Good practices

- Regulate the procurement relations via a contract signed intuitu personæ.
- Require the processor to forward its Information Systems Security Policy (PSSI) along with all supporting documents of its information security certifications and append said documents to the contract. Ensure that the measures pursuant to its PSSI comply with the CNIL's recommendations in this respect.
- Precisely determine and set, on a contractual basis, the operations that the processor will be required to carry out on personal data:
  - ♦ The data to which it will have access or which will be transmitted to it.
  - ♦ The operations it must carry out on the data.
  - ♦ The duration for which it may store the data.
  - ♦ Any recipients to which the data controller requires it to transmit the data.
  - ♦ The operations to be carried out at the end of the service (permanent deletion of data or return of the data in the context of reversibility then destruction of data at the processor's).

- ♦ The security objectives set by the data controller.

- Determine, on a contractual basis, the division of responsibility regarding the legal processes aimed at allowing the data subjects to exercise their rights.
- Explicitly prohibit or regulate use of tier-2 processors.
- Clarify in the contract that compliance with the data protection obligations is a binding requirement of the contract.

34.3 Specific measures for providers of cloud computing services

Good practices

In addition to the good practices applicable in the event a processor is used, the following measures may be implemented:

- Require the provider to apply at least logical separation between the organization's data and the data of its other clients.
- Very clearly define the locations in which the data are likely to be stored, and the countries from which the data stored in the cloud are likely to be accessible.
  - ♦ *Recommendation: cloud computing service providers often stipulate the data storage location, but seldom indicate the geographic regions from which their administrators access their platform; this point must be clarified in the contract.*
- See the CNIL's recommendation on cloud computing

35 Supervision

Aims: to get a comprehensive and up-to-date view of data protection and compliance with the DP-Act (check the compliance of processing operations, objectives and indicators, responsibilities, etc.).

Good practices to be followed if the measure is used to address risks

- Regularly inspect personal data processing operations to ensure that they comply with the DP-Act as well as the effectiveness and appropriateness of planned measures.
  - ♦ *Recommendations: perform checks of the most sensitive processing operations and of operations which are the subject of personal data breaches or complaints, at random so that all operations are inspected on a regular basis; have a third party perform occasional audits, particularly of the most sensitive processing operations.*
- Set data protection objectives and define indicators for determining whether these objectives are met.
  - ♦ *Recommendations: have a map of personal data processing operations and the associated risks, give prior notification to the CNIL for all processing operations prior to their implementation, etc.*
- Determine the respective responsibilities based on the risks connected to the personal data.
  - ♦ *Recommendations: establish a "RACI matrix;" that is, determine who is responsible for carrying out each action (R=Responsible), who is accountable (A=Accountable), who is consulted (c=Consulted) and who is kept informed (I=Informed).*
- Regularly assess data protection.
  - ♦ *Recommendations: present the controller with an annual map of risks to all processing operations, an annual assessment of compliance with the data protection policy, a progress report on planned actions, etc.*

Tools/ To find out more

- The CNIL approves data protection audit procedures.
- To find out which formalities are carried out beforehand by your organization with the CNIL, send a fax requesting the "Article 31" list and indicating the SIREN number and address of your organization to + 33 (0)1 53 73 22 00.
- See the guide to drawing up information system security management charts (TDBSSI) which ANSSI has put online.

36 Surveillance

36.1 General measures

Aims: to allow early detection of incidents involving personal data and to have information that can be used to analyze them or provide proof in connection with investigations (logging policy and architecture, compliance with personal data protection obligations, etc.).

Good practices to be followed if the measure is used to address risks

- Set up a logging architecture that retains a record of security incidents and the time they occurred.
  - ♦ *Recommendations: date- and timestamp the logged incidents based on UTC time (Coordinated Universal Time), use a reliable time source (such as an NTP (Network Time Protocol) server or radio synchronization) to synchronize the equipment, centralize locally (assemble all the logs on a relatively isolated collection machine supported by a dedicated consultation workstation), export the logs (scheduled dispatches, automatic transfer or an administration network), provide for sufficient storage capacity, set up an archiving and backup system for the incident logs, protect the logging equipment and the information logged against sabotage and unauthorized access, etc.*
- Select the incidents to be logged based on the context, supporting assets (including workstations, firewall, network equipment and servers), risks and legal framework.
  - ♦ *Recommendations: log the actions on the workstations only in the case of heightened risks; comply with the French Postal and Electronic Communications Code if public Internet access is set up (only store connection data for one year if they are collected in connection with the service, information allowing the user and the recipient(s) of the communication to be identified, data on the communication terminal equipment used, technical features, the date, schedule and duration of each communication and data on the additional services requested or used and their suppliers), with a strict duty of confidentiality, comply with the LCEN Decree.*
    (Act on Confidence in the Digital Economy) if content is created online (only store for one year if they are collected in connection with the service: connection data, content creation data, contract-related data and payment-related data, etc.
- Comply with the requirements of the DP-Act if the logged events include personal data.
  - ♦ *Recommendations: users must be informed of the systems used, those systems' use must be declared to the CNIL and the use of the data collected must comply with the purpose stated initially.*

- Conduct periodic analyses of the logged information, and if needs be establish a system that detects weak signals automatically.
- Retain the incident logs for six months unless legal and regulatory restrictions require specific storage durations.

Tools/ To find out more

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

36.2 Specific measures for a client workstation

Good practices to be followed if the measure is used to address risks

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

36.3 Specific measures for a firewall

Good practices to be followed if the measure is used to address risks

- Establish a filtering policy that prohibits any direct communication between the internal workstations and the exterior (permit connections only via the firewall) and allow only those flows that are explicitly authorized (firewall blockage of all connections except those identified as necessary).
- Log all successful authorized connections and all rejected attempts to connect.

- ♦ *Recommendations: for each connection, time- and datestamp the logs to the nearest millisecond, log, at a minimum, the source and destination IP addresses, the transport protocol and the flags and connection states associated with the segments for the TCP protocol.*

- Export the logs via a secure channel to a dedicated server.

36.4 Specific measures for network equipment

Good practices to be followed if the measure is used to address risks

- Log the activity on each port of a switch or a router.
- Export the logs to a dedicated server using an integrated client syslog or via a netflow.
- Monitor the volume based on times and monitor compliance with any access control lists (ACL) for the routers.

36.5 Specific measures for a server

Good practices to be followed if the measure is used to address risks

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

37 Operating security

Aims: to limit the likelihood and severity of risks targeting the supporting assets used in operation (document the operating procedures, inventory and update of software and hardware, correction of vulnerabilities, duplication of data, limit physical access to the hardware, etc.).

Good practices to be followed if the measure is used to address risks

- Document the operating procedures, update them and make them available to all users concerned (every action on the system, whether it involves administration operations or the use of an application, must be explained in the users' reference documents).
- Maintain an up-to-date inventory of the software and hardware used in operation.
  - ♦ *Recommendations: keep an exhaustive list of software, physical and virtual servers, infrastructure components, services managed by third parties and networks and telecommunications equipment used for carrying out the personal data processing. Include in this list the information about the equipment, the type of operating system, the network (IP address, MAC address), the applications used, the present versions and the patches installed, and the versions of firmware for equipment for which these can be updated).*
- Conduct monitoring of vulnerabilities discovered in the software (including firmware) used in operation, and correct them at the earliest possible opportunity.
  - ♦ *Recommendations: to the extent possible, activate the software automatic update systems. When this is not possible, install corrective updates as soon as they become available. Otherwise set up mechanisms aimed at preventing the use of any vulnerabilities discovered.*
- Formally document hardware and software update procedures.
- Prohibit the use of production servers (database servers, Web servers, messaging server, etc.) for other purposes than those initially intended
  - ♦ *Recommendations: only install software that is absolutely necessary on the servers, limit network traffic to ports that are absolutely necessary.*
- Use data storage units that use physical redundancy mechanisms (such as RAID), or mechanisms for duplicating data between several servers and/or sites.
- Check that the size of storage and computing capacities is sufficient for allowing the processing to operate correctly – even during activity peaks.
- Check that the physical hosting conditions (temperature, humidity, energy supply, etc.) are compatible with the intended use of hardware, and include backup mechanisms (inverter and/or backup supply and/or generator).
- Limit access to hardware that is sensitive and/or of high market value.
- Limit the possibilities of hardware alteration.

- ♦ *Recommendations: use security seals to determine whether computers have been opened, padlock machine system units when this is possible, lock disk arrays.*

- Provide for an Activity Recovery Plan (PRA) or Activity Continuity Plan (PCA), based on the availability objectives of the processing carried out.
  - ♦ *Recommendations: formally document the PRA or PCA, disseminate it among the staff concerned (internal, external and service providers), and regularly test its effectiveness.*
- Set up a security incident management procedure allowing such incidents to be detected, recorded, described and resolved (see the page Management of incidents and data breaches).

38 Security of computer channels (networks)

38.1 General measures

Aims: to reduce the possibility that the characteristics of IT channels (wired networks, Wi-Fi, radio waves, fiber optics, etc.) can adversely affect personal data (network mapping, firewall, intrusion prevention and detection, SSH protocol, flow encryption, strong authentication, etc.).

Good practices to be followed if the measure is used to address risks

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

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

Tools/ To find out more

- Network activity may be monitored with the help of:
    - ♦ intrusion detection systems (either NIDS, which monitor networks for security breaches, or HIDS, which monitor the security of network-connected computers, or hybrid IDS);
    - ♦ intrusion prevention systems (either NIPS, which monitor entire networks for suspicious traffic by analyzing protocol activity, or WIPS, which monitor wireless networks for suspicious traffic by analyzing wireless networking protocols, or NBA, which identify threats that generate unusual traffic flows, or HIPS, which monitor hardware for unusual activity).
- See the briefing notes CERTA Filtering, CERTA SSL, CERTA Hoaxes, CERTA Spam, CERTA Tunnels, CERTA Indexing, CERTA PHP, CERTA IPv6, CERTA DNS and CERTA Backscatting.
- See the "Authentication" function requirements in the General Security Framework (RGS).

38.2 Specific measures for connections to active network hardware

Good practices to be followed if the measure is used to address risks

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

38.3 Specific measures for remote-administration tools

Good practices to be followed if the measure is used to address risks

- Restrict the remote administration of local IT resources to IT department staff and to IT resources within the limits of their duties.
- Uniquely identify users of remote-administration tools.
- Authenticate users of remote-administration tools with at least a robust password and, where possible, a digital certificate.
- Keep a log of the activity of users of remote-administration tools (see the page Traceability (logging)).
- Secure the secure authentication flow.
    - ♦ *Recommendations: no clear-text passwords, no replayable sequences, etc.*
- Remote administration must be covered by prior agreement on the part of the user.
    - ♦ *Recommendations: clicking a pop-up.*
- Prohibit changes to the tool's security settings and the viewing of passwords or secret information used.
- Block the retrieval of secret information for the purposes of establishing a connection from a workstation.
- Encrypt all traffic flows.
- The user must be informed that remote administration is under way on his/her workstation (for example via an icon).

38.4 Specific measures for mobile or remote devices

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

Good practices to be followed if the measure is used to address risks

- Where possible, set up a strong solution for authenticating users who access internal information systems (when this is possible).
    - ♦ *Recommendations: require at least two distinct authentication factors from among something a user knows (e.g. a password, OTP tokens, without forgetting to change default activation passwords), something a user has*

(e.g. a digital certificate, smart card) and a characteristic specific to the individual (e.g. a fingerprint, other biometric identifiers).

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

38.5 Specific measures for wireless interfaces (Wi-Fi, Bluetooth, infrared, 4G, etc.)

Good practices to be followed if the measure is used to address risks

- Prohibit non-secure communications for connections via wireless interfaces.
- Prohibit simultaneous network connections via a wireless interface and the Ethernet interface.
- Disable unused wireless connection interfaces (Wi-Fi, Bluetooth, infrared, 4G, etc.) on hardware and software.
- Control wireless networks.
  - ♦ *Recommendations: only authorize wireless infrastructures that allow staff to access local resources (extension of the LAN) and public Internet access that is completely isolated from the organization's LAN infrastructure, authenticate users, encrypt traffic, etc.*

38.6 Specific measures for Wi-Fi

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- See the CERTA-Wi-Fi briefing note.

- See the specific practical guide for setting up Wi-Fi access of the ASIP
- MAC address filtering may be used in certain cases to protect Wi-Fi access.

38.7 Specific measures for Bluetooth

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- See the CERTA-Bluetooth briefing note.

38.8 Specific measures for infrared

Good practices to be followed if the measure is used to address risks

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

38.9 Specific measures for mobile telephony networks (2G, 3G or 4G, etc.)

Good practices to be followed if the measure is used to address risks

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

38.10 Specific measures for Web browsing

Good practices to be followed if the measure is used to address risks

- Use the SSL protocol (HTTPS) to ensure server authentication and confidentiality of communications.
- Favor keys generated in accordance with the RGS.
- ♦ *Recommendations: contract with an electronic certificate service provider that complies with Version 1.0 of the RGS for server authentication use .*

38.11 Specific measures for file transfers

Good practices to be followed if the measure is used to address risks

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

38.12 Specific measures for fax machines

Good practices to be followed if the measure is used to address risks

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

38.13 Specific measures for ADSL/Fiber

Good practices to be followed if the measure is used to address risks

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

38.14 Specific measures for email

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- Define a policy for managing email authentication and use the DMARC protocol (*Domain-based Message Authentication, Reporting and Conformance*) to reduce abuse thereof.

38.15 Specific measures for instant messaging

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- See the CERTA-IRC briefing note.

39 Paper document security

Aims: limit the risks of unauthorized persons accessing paper documents containing personal data (indication of classification, printing processes, restricted dissemination, traceability of transmissions, etc.).

39.1 Marking documents that contain personal data

Aims: to encourage cautious behavior among individuals with access to documents by clearly identifying those that contain personal data.

Good practices to be followed if the measure is used to address risks

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

Notes

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

39.2 Reducing the vulnerabilities of paper documents

Aims: to reduce the possibility of paper document characteristics being used to adversely affect personal data.

Good practices to be followed if the measure is used to address risks

- Choose paper formats and printing methods that are suitable to the storage conditions (storage duration, ambient humidity, etc.).
- Retrieve printed documents containing personal data immediately after they are printed or, where possible, carry out secure printing.
- Restrict the distribution of paper documents containing personal data to individuals who require them for work-related purposes.
- Store paper documents containing personal data in a secure cabinet.
  - ♦ *Recommendations: store them in a fireproof file cabinet with key lock, a safe, etc.*
- Destroy, using a shredder of the appropriate certification level, paper documents that are no longer necessary and which contain personal data.
  - ♦ *Recommendations: The German DIN 32757 standard defines five shredder security levels based on document sensitivity: use a shredder certified at least level 3.*

Tools/To find out more

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

39.3 Reducing the vulnerabilities of paper channels

Aims: to reduce the possibility of paper channel characteristics (circulation within an organization, delivery by vehicle, mail delivery, etc.) being used to adversely affect personal data.

Good practices to be followed if the measure is used to address risks

- Only send paper documents containing personal data that are necessary for processing.
- Keep close track of the circulation of paper documents containing personal data.
  - ♦ *Recommendations: keep a specific record of all documents containing personal information that are sent (list of documents sent, sender's identity and signature, transmission channel, truck driver's/courier's identity and signature, date and time of sending) or received (list of documents received, recipient's identity and signature, date and time of receipt), etc.*
- Choose a transmission channel that is suited to the risks and frequency of transmission.

♦ *Recommendations: use the postal service, the organization's own services (vehicles and drivers) or a package delivery company, etc.*

- Improve trust in companies used to deliver paper documents containing personal data.
  - ♦ *Recommendations: inform people who deliver paper documents about the risks involved if the documents belong to the organization, draw up clauses on protecting the availability, integrity and confidentiality of paper documents in agreements with package delivery companies, verify the identity of truck drivers/couriers, etc.*
- Protect paper documents containing personal data.
  - ♦ *Recommendations: send documents by registered mail inside two envelopes, mark the envelopes as "Confidential", use envelopes, boxes or other containers that withstand threats from sources other than people (accidents, fires, etc.), etc.*

Tools/ To find out more

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

40 Hardware security

40.1 General measures

Aims: to reduce the possibility of hardware characteristics (servers, desktop computers, laptops, associated devices, communications relays, removable storage devices, etc.) being used to adversely affect personal data (inventory, partitioning, physical redundancy, restrict access, etc.).

Good practices to be followed if the measure is used to address risks

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

40.2 Specific measures for workstations

Good practices to be followed if the measure is used to address risks

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

40.3 Specific measures for mobile devices

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

Good practices to be followed if the measure is used to address risks

- Encrypt the data stored on mobile devices in line with the measures recommended on the page Encryption.
    - ♦ *Recommendations: physically encrypt the entire hard disk, logically encrypt the entire hard disk via the operating system or another software, encrypt files individually, create encrypted containers, etc.*
- Limit the amount of personal data stored on mobile devices to the strict minimum, and prohibit such storage during travel abroad if needs be.
- Ensure the availability of personal data stored on mobile devices.
    - ♦ *Recommendations: copy personal data to another computer or another server as soon as possible, etc.*
- Erase personal data from mobile devices as soon as such data are entered in the organization's information system.
- Place privacy filters on mobile devices whenever they are used outside the organization.
- Configure devices so that they lock after a few minutes of inactivity.

Notes

- More and more laptops are equipped with fingerprint readers. The use of such readers is subject to authorization from CNIL unless they are covered under the Single authorization 52.
- Users must not be able to disable disk encryptions; ensure that a copy of the keys is retained when encryption is used.

Tools/ To find out more

- See the ANSSI guide for travel abroad.

40.4 Specific measures for removable storage devices

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

Good practices to be followed if the measure is used to address risks

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

Tools/ To find out more

- See the CERTA briefing note on risks associated with USB flash drives.

40.5 Specific measures for multifunction printers and copiers

Good practices to be followed if the measure is used to address risks

- Change "manufacturer" default passwords.
- Disable unnecessary network interfaces.

- Disable or delete unnecessary services.
- Encrypt data stored on hard disks wherever possible.
- Restrict the sending of electronic documents to internal email addresses and, in certain cases, restrict the sending of electronic documents to a single email address.
- If maintenance is performed by a third party, set up measures to block access to personal data.
    - ♦ *Recommendations: data must be either securely encrypted or erased before hardware is sent out for maintenance; have the maintenance company sign a confidentiality agreement or have the repairs performed on-site in the presence of a member of the IT department where data are sensitive and cannot be completely encrypted or erased (hard disk failure, malfunction, etc.); prohibit hardware containing sensitive data from being sent out for maintenance, etc.*
- If a locally networked multifunction printer or copier is maintained remotely by a third party, take specific measures to protect access to this equipment.
    - ♦ *Recommendations: have the external third party sign a confidentiality agreement, use individual robust passwords that are changed on a regular basis, enable dial-in access for remote maintenance purposes only when requested, dial-in access should be disabled by default, keep a remote maintenance access log, prohibit the possibility of using remote maintenance to bounce to the rest of the LAN and the Internet, etc.*
- Block access to personal data stored on discarded multifunction printers or copiers.
    - ♦ *Recommendations: store equipment on-site in a secure room until it is taken away, use a secure erasing tool to wipe data from hard disks or built-in memory. If wiping is not possible (due to failure, malfunction, etc.), physically destroy equipment. If equipment disposal is contracted out, have the disposal company sign a confidentiality agreement. Issue an equipment destruction report and retain it for 10 years.*

41 Website security

Aims: reduce the possibility of website characteristics being used to adversely affect personal data (general security framework, TLS encryption of traffic, cookie installation policy, security audits, etc.).

Good practices to be followed if the measure is used to address risks

- If the website is a teleservice, this must comply with the General Security Framework (RGS). For that, the website must particularly use a certificate signed by an "approved" trusted root authority (e.g.: LSTI, see the list of approved electronic certification service providers);
  - ♦ *Recommendation: the RGS compliance certificate must be available on the website.*
- Traffic encryption must be guaranteed by TLS; then, it is necessary to configure the web server so that this only accepts this type of protocol (particularly exclude the SSL protocol and render encryption compulsory during SSL negotiations)
- If you use cookies:
  - ♦ Make sure you have obtained consent prior to their installation, ♦ For cookies installed from your domain:
    - ◊ Make sure you limit the validity term of cookies to 13 months,
    - ◊ Use the HTTP-ONLY flag,
    - ◊ Use the Same-Site flag for cookies that do not need to be accessible from third-party premises.
- Define a Content-Security-Policy only including stakeholders whom you authorize to place content on your website.
- Conduct on-site security audits.

Tools/ To find out more

- The French Network and Information Security Agency (ANSSI) has provided a guide on this subject; you are advised to follow the recommendations therein.

42 Transfers: compliance with the obligations bearing on transfer of data outside the European Union

Aims: to comply with Articles 68 and 69 of the DP-Act and Articles 44 to 50 of the General Data Protection Regulation (GDPR); comply with the obligations bearing on transfer of data outside the European Union.

Good practices

- State the geographic storage location for the different types of processing data.
- Depending on the country in question, justify the choice of remote hosting and indicate the legal supervision arrangements implemented in order to ensure adequate protection of the data which are subject to a cross-border transfer.

43 Traceability (logging)

Aims: to ensure that consultation and action carried out by users of the processing are recorded and attributed, such that it is possible to provide evidence during investigations (logging system, protection, analysis, storage, etc.).

Good practices to be followed if the measure is used to address risks

- Set up an applicative logging system that retains a record of data modifications and access carried out by the users and the time they took place.
  - ♦ *Recommendations: date- and timestamp the logged incidents based on UTC time (Coordinated Universal Time), use a reliable time source (such as an NTP (Network Time Protocol) server or radio synchronization) to synchronize the equipment, centralize locally (assemble all the logs on a relatively isolated collection machine supported by a dedicated consultation workstation), export the logs (scheduled dispatches, automatic transfer or an administration network), provide for sufficient storage capacity, set up an archiving and backup system for the incident logs, protect the logging equipment and the information logged against sabotage and unauthorized access, ensure the strict confidentiality of logs, etc.*
- Set up user authentication making it possible to attribute the logged incidents.
  - ♦ *Recommendations: prohibit generic or shared identifiers, comply with the CNIL's recommendations on passwords, give precedence to strong, two-factor authentication, etc.*
- Comply with the requirements of the DP-Act as regards logged events attached to an identified user.
  - ♦ *Recommendations: it is necessary to inform users of the traceability set up, include this in the processing declaration to the CNIL and not to use the records collected for other purposes, etc.*
- Conduct periodic analyses of the logged information and, if needs be, establish a system that detects abnormal activity automatically.
- Retain the event logs for six months unless legal and regulatory restrictions require specific storage durations.

Tools/ To find out more

- Based on the analysis of risks and legal requirements, ensure the probative value of the logs via technical measures (date- and timestamping, digital signature, device fingerprinting) in line with the General Security Framework (RGS).