Privacy Impact Assessment (PIA)

APPLICATION TO IOT DEVICES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

February 2018 edition

Contents

Foreword

This document is an application of the PIA guides published by the CNIL to the specific sector of the IoT devices (connected objects).

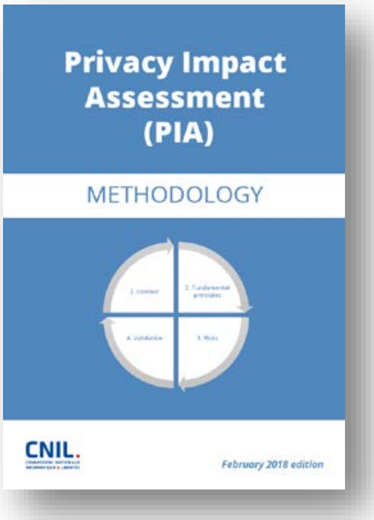
Performed in principle by a controller or provider, the purpose of a PIA is to build and demonstrate the implementation of privacy protection principles so as to empower data subjects.

This is an iterative methodology, which should guarantee a reasoned, reliable use of such data during processing.

This document is based upon the PIA method of the French Data Protection Authority (CNIL)

The methodology comprises three guides, one setting out the approach, a second containing facts that could be used for formalizing 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 website and will be useful for completing this document:



Privacy Impact Assessment (PIA)

METHODOLOGY

CNIL.

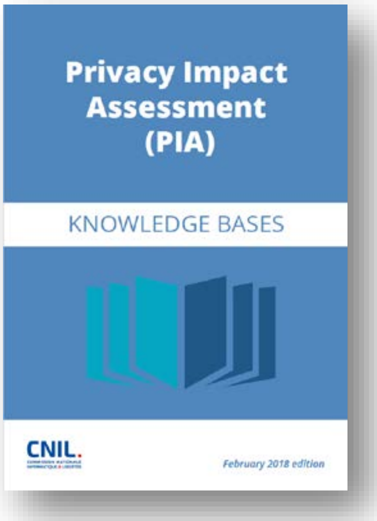
February 2018 edition

Privacy Impact Assessment (PIA)

TEMPLATES

CNIL.

February 2018 edition



Privacy Impact Assessment (PIA)

KNOWLEDGE BASES

CNIL.

February 2018 edition

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

This document is laid out like a PIA report – the deliverable of the PIA[1].

Some parts of this document [grey shaded areas] have been filled in for illustrative purposes, taking as an example a fictional generic product comprising an interactive toy which can also be used as a babyphone, a mobile app and an online service, for which personal data are stored by a third-party hosting provider which calls on service providers (interactivity, analysis of uses, advertising company).

In addition, there are notes giving advice or highlighting points to be vigilant about in the specific context of connected objects.

Lastly, insets [beige areas] provide methodological support throughout the document to inform the planned assessments.

[1] See the WP29 guidelines on PIAs.

1 Study of the context

Generally carried out by the project owner[2], with the help of a person in charge of “Data protection” aspects[3].

Objective: gain a clear overview of the personal data processing operations under consideration.

1.1 Overview of the processing

- Present a brief outline of **the product** under consideration, its **nature**, **scope**, **context**, **purposes** and **stakes** [4]
- Identify the **data controller** and any **processors**.
- List the **references applicable** to the processing, which are necessary or must be complied with[5], not least the approved codes of conduct (see Art. 40 of the [GDPR]) and certifications regarding data protection (see Art. 42 of the [GDPR])[6].

1.1.1 Product description

The template below can be used to provide a brief description of the product.

To show how to use it, it has been completed taking the example of a fictional toy, which will be used throughout the document.

Product description	The device is a toy fitted with a microphone, a camera and basic functional buttons (power, action, reset). It connects via Wi-Fi and communicates with a dedicated mobile app, hosted on a smartphone or a tablet, or with an online service.
Processing purposes	Provide interactivity to the child, through the possibility of dialogue with the toy (questions/answers in natural language by voice recognition). Enable the child to communicate online (send voice messages, texts and photos) with his/her friends and/or parents. Feed information back to the parents (surveillance device).
Processing stakes	Create a new category of toys for children and their parents by leveraging connectivity, in keeping with the legal framework and personal data security.
Controller	The firm *Fab* (manufacturer)
Processor(s)	The firms *Héb* (host), *Int* (interactive platform) and *AnaPub* (analysis of uses and advertising company)

[2] In the business sense. This may be delegated, represented or processed by another stakeholder.

[3] Such as the data protection officer for example.

[4] Answer the question "What are the expected benefits (for the organization, for the data subjects, for society in general, *etc.*)?"

[5] Depending on the case, they will particularly be useful to demonstrate compliance with fundamental principles, justify controls or prove that they correspond to the state of the art.

[6] Other examples: security policy, sector-specific legal standards, *etc.*

1.1.2 Sector-specific references applicable to the processing[7]

Below you will find a table setting out the sector-specific standards applicable to your processing[8] along with the conditions for taking them into account.

Standards applicable to the processing	Consideration

1.2 Data, processes and supporting assets

- ❑ Define and describe the scope in detail:
  - o the personal **data** concerned, the **recipients**[9] and **storage durations**;
  - o description of the **processes** and personal data **supporting assets** for the entire personal data life cycle (from collection to erasure).

1.2.1 Data processed

Below you will find a table setting out a detailed list of the data processed and persons with access thereto.

To show how to use it, it has been completed with the data from our example of a fictional toy.

Personal data	Categories	Recipients	Persons with access thereto
Information about the user: first name, date of birth, gender, email, telephone number	Common data: identification data	The firm *Héb*	Authorized staff at the firms *Fab* and *Héb*
Data entered in a third-party app (Twitter, Facebook, *etc.*), obtained via a link with the user account	Common data: identification data	The firm *Héb*	Authorized staff at the firms *Fab* and *Héb*
Recorded data: texts/messages, sounds, images, movements, temperature, humidity User logs on the device, mobile app and online service	Common data: life habits Data perceived as sensitive: image and voice (enabling biometric processing) Sensitive data (in the meaning of the GDPR): data relating to minors	The firm *Héb* + The firms *Int* and *AnaPub*	Authorized staff at the firms *Fab* and *Héb* + Authorized staff at the firms *Int* and *AnaPub*
Calculated data: answers to children's questions and identification of interests to help make answers more relevant	Common data: life habits	The firms *Int* and *AnaPub* +	Authorized staff at the firms *Int* and *AnaPub*

[7] See Article 35 (8) of the [GDPR].

[8] For example a code of conduct, a certification, a general security policy or a PIA Framework.

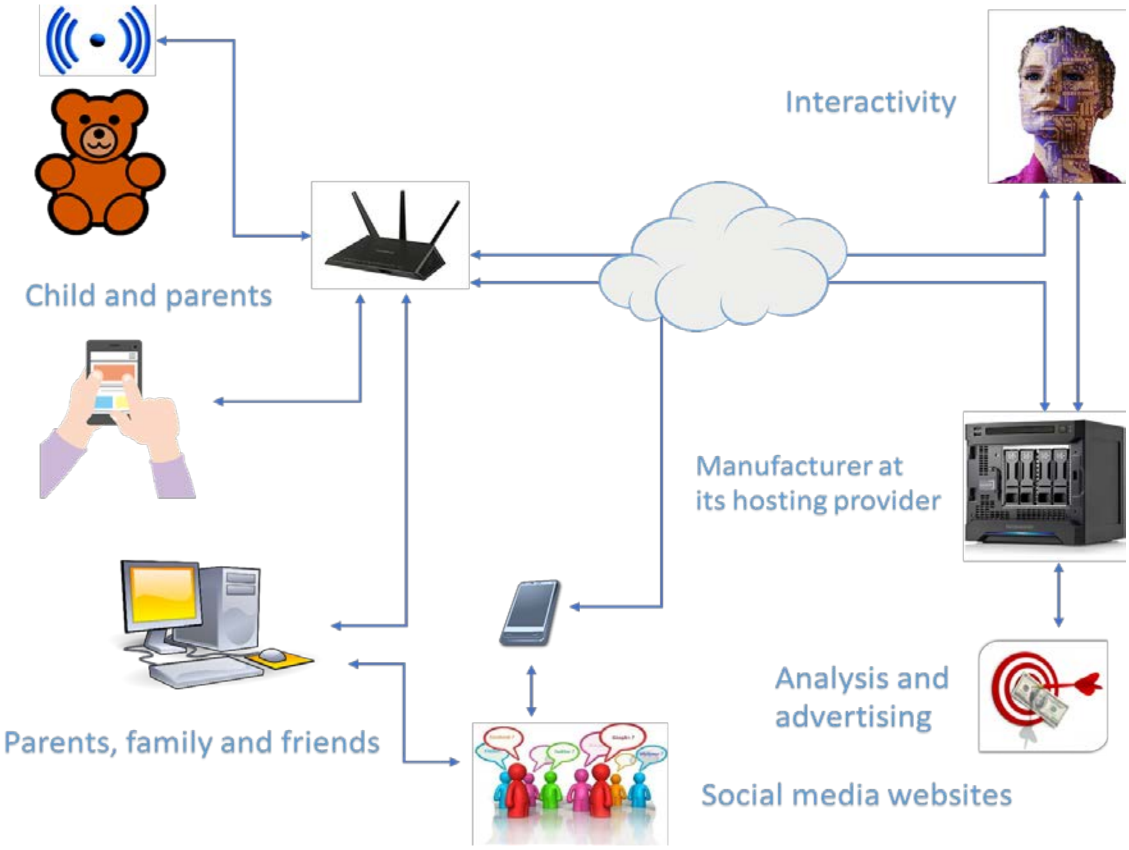
[9] For the definition of "recipient", see Article 4(9) of the GDPR.

Personal data	Categories	Recipients	Persons with access thereto
Analysis of uses and targeted advertising	Sensitive data (in the meaning of the GDPR): data relating to minors	The firm *Héb*	+ Authorized staff at the firms *Fab* and *Héb*

1.2.2 Life cycle of data and processes

Here you need to present and describe how the product generally works, with a diagram of data flows and a detailed description of the processes carried out.

As an example, below you will find the diagram showing how our fictional toy works.



Below you will find a table for listing in detail all the data processing operations carried out.

To show how to use it, it has been completed with our example of a fictional toy.

Processes	Detailed description of the process
1. Open an account	The user provides identification data to open his or her account
2. Capture the data	Data are recorded via sensors
3. Transfer to the mobile	The data are transferred to the mobile app, directly via the device or through the cloud servers
4. Enter the data	Data are entered into the mobile app
5. Store in the mobile	The data are stored in the mobile app
6. Send the data to the servers	The data are sent to the cloud servers, via the device directly or the mobile app
7. Generate interactivity	The interactive platform in the cloud generates the response data on the basis of previous dialogues and the interests detected
8. Send the data to the toy	The interactive data are sent back to the device, directly or through the mobile app
9. Store the data on the servers	The captured and calculated data are stored on the cloud servers
10. Analyze the data	Data analysis algorithms are run on the cloud servers to produce statistics on use and advertising targeting
11. Consult the cloud server data	Part of the captured and calculated data can be consulted via the mobile app or on a personal Web space
12. Share the data	Some data can be passed on to third-party apps or posted on social media websites

1.2.3 Data supporting assets

Below you will find a table for listing in detail the data supporting assets. To show how to use it, it has been completed with our example of a fictional toy.

IT systems[10] on which the data rely	Other supporting assets[11]
- Device (camera, microphone, loudspeaker, movement sensors, temperature, humidity) - Smartphone/tablet/computer of the user - Mobile app/browser - Wi-Fi network - Internet - Cloud servers of *Héb, Int and AnaPub*	- User - User's premises - Premises of *Fab* and *Héb* - Staff at *Fab* and *Héb* - Premises of *Int* and *AnaPub* - Staff at *Int* and *AnaPub*

NB: the whole of Part 1 "Context" must be read through by the DPO to make sure that it is exhaustive and properly reflects the way things really are.

This is all the more necessary given that this part describes the key aspects and notions on which the following chapters are based.

[10] Can be broken down into hardware (and electronic data media), software and computer channels.
[11] Can be broken down into people, paper documents and paper transmission channels.

2 Study of the fundamental principles

Generally performed by the project owner and then assessed by a person in charge of "Data Protection".

Objective: build the system that ensures compliance with privacy principles.

The fundamental principles bearing on privacy protection which must be taken on board are as follows: specified and explicit data collection purposes, lawfulness of the processing, data minimization, data quality, limited storage durations, information for the data subjects, obtaining their consent, possibility of accessing their data directly, portability of their data, possibility of rectifying and erasing their data at their request, possibility of objecting to or restricting the processing, regulation of processors and transfer of data outside the European Union.

- ❑ Explain and justify the **choices made** and describe the **controls selected** (existing or planned) **to comply with these legal requirements** (it is necessary to explain how it is intended to implement them).
- ❑ Check that improving the way in which each point is planned, clarified and justified, pursuant to the [GDPR], is either not necessary or not possible.
- ❑ Where applicable, review their description or propose additional controls.

Note: In Para. 2.3 below, you will find a table for summarizing the justifications for all these points and for recording their assessment and any corrective controls.

2.1 Controls guaranteeing the proportionality and necessity of the processing

2.1.1 Purposes: specified, explicit and legitimate[12]

Below you will find a table for setting out in detail the data processing purposes and for justifying their legitimacy[13].

Purposes	Legitimacy

Note: remember to explain the purposes of sharing with third parties, in particular for advertising and "partner offers", as well as the data processing purposes for improving the service.

Note: remember to explain the specific conditions under which the processing will take place, particularly by clarifying data matching where applicable.

[12] See Article 5.1 (b) of the [GDPR].

[13] On the legitimacy of the purpose, see opinion WP 203 of the Article 29 Data Protection Working Party - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

NB[14] : on account of a child's general vulnerability and the fact that personal data must be processed fairly and lawfully, the controllers of a processing operation targeting children must comply even more strictly with the principles of purpose limitation.

More particularly, the controllers must not use the child's data for profiling purposes (e.g. for targeted advertising), whether directly or indirectly, insofar as it is not possible for a child to understand the implications of this, and it therefore goes beyond what can be considered fair processing.

2.1.2 Basis: lawfulness of processing, prohibition of misuse[15]

Below you will find the list of lawfulness criteria. Processing shall be lawful only if and to the extent that at least one of the following applies:

Lawfulness criteria	Applicable	Justification
The data subject has given consent [16] to the processing of his or her personal data for one or more specific purposes		
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		
Processing is necessary for compliance with a legal obligation to which the controller is subject		
Processing is necessary in order to protect the vital interests of the data subject or of another natural person		
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		
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[17]		

Note: 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.

Note: 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, *etc.*) 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

[14] See the WP29 opinion 02/2013 on apps on smart devices.

[15] See article 6 of the [GDPR].

[16] With regard to obtaining the data subject's consent and informing the latter, see Chapter 2.2.

[17] This point shall not apply to processing carried out by public authorities in the performance of their tasks

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[18];
- ❑ the possible consequences of the intended further processing for data subjects;
- ❑ the existence of appropriate safeguards, which may include encryption or pseudonymization.

2.1.3 Data minimization: adequate, relevant and limited [19]

It is important to reduce the severity of the risks by minimizing the number of personal data that will be processed, by limiting such data to what is strictly necessary for the purposes for which they are processed (otherwise they should not be collected). Then, it also becomes possible to minimize the data themselves, via controls aimed at reducing their sensitivity (see Appendix 1 - List of data minimization controls).

Below you will find a table for listing the data processed, reduced to what is strictly necessary, alongside the justification of the need and any additional minimization controls.

To show how to use it, it has been completed with the data from our example of a fictional toy.

Data types	Data categories	Details about the data processed	Justification of the need and relevance of the data	Minimization controls
Common data	Civil status, identity, identification data	First name, date of birth, email, telephone number, link with a social media account	Details necessary for creating a profile for communicating	No surname Replacing the date of birth with the age or age group Separate storage of identifying data in an encrypted base
	Personal life (living habits, marital status, excluding sensitive or dangerous data, *etc.*)	Texts/messages, sounds, images, movements, temperature, humidity Answers to children's questions and identification of interests to help make answers more relevant, targeted advertising	Aspects that are part of the communication features	
	Professional life (résumé, education and professional training, awards, *etc.*)	Not collected		

[18] See Articles 9 and 10 of the [GDPR].

[19] See Article 5.1 (c) of the [GDPR].

Data types	Data categories	Details about the data processed	Justification of the need and relevance of the data	Minimization controls
	Economic and financial information (income, financial situation, tax situation, *etc.*)	Not collected		
	Connection data (IP addresses, events logs, *etc.*)	Application traces Technical logs	Required for security reasons and to check compliance with the ST&Cs	Pseudonymization for statistical use
	Location data (travels, GPS data, GSM data, *etc.*)	Smartphone location integrated in the photos (if option is activated)	Not necessary	Removal of location information before photos are sent
Data perceived as sensitive	Social security number	Not collected		
	Biometric data	Raw data: voice and photographs	Aspects that are part of the communication features	
	Bank data	Not collected		
Sensitive data in the meaning of the [DP-Act][20]	Opinions bearing on philosophy, politics, religion, trade union involvement, sexuality, health data, racial or ethnic origin, data concerning health or sexuality	Not collected but can appear directly or indirectly in the text, audio and video data	Aspects that are part of the communication features	
	Offences, convictions, security measures	Not collected		

Notes: remember to clearly justify the collection of certain data (location, date of birth, age, weight, *etc.*) and clearly distinguish between anonymous and pseudonymous data.

Tip: avoid free text input fields (like "comments" fields), because of the risk of users noting down there information that does not comply with the minimization principles. 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.*).

NB: for processing of minors' details, the data are considered overall to be sensitive pursuant to the [GDPR].

[20] Also see Articles 9 & 10 of the [GDPR]. Restrictions of use and special formalities are to be taken into account.

NB[21] : on account of a child's general vulnerability and the fact that personal data must be processed fairly and lawfully, the controllers of a processing operation targeting children must comply even more strictly with the principles of data minimization and purpose limitation.

The data controllers should also specifically refrain from any collection of data relating to the parents or family members of the child user, such as financial information or information about special categories of information, such as medical data.

2.1.4 Quality of data: accurate and kept up-to-date[22]

Below you will find a table for setting out in detail the data quality compliance controls, carried out on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

Data quality controls	Device	Mobile app	Personal account	Justification
Regular checks of the accuracy of the user's personal data				
Invitation for the user to check and, where necessary, update his or her data				
Traceability of data amendments				

2.1.5 Storage durations: limited[23]

A storage duration must be defined for each type of data and justified by the legal requirements and/or processing needs. Thus a distinction is made between common data and archived data, to which access will be limited to only the stakeholders concerned.

An erasure mechanism must be implemented to archive common data or purge archived data at the end of their storage duration. Functional traces will also have to be purged, as will technical logs which may not be stored indefinitely.

Notes: By reducing the amount of available and processed data, archiving and purging help to limit the impacts in the event of theft or accidental dissemination of the database.

In order to ensure that these storage durations are effective, it is recommended to set up an automatic mechanism based on the date on which the data are created or last used.

NB: For sensitive data and high-risk data, use should be made of secure erasure tools that make the data irretrievable.

[21] See WP29 opinion 02/2013 on apps on smart devices.

[22] See Article 5.1 (d) of the [GDPR]). The quality requirement also concerns the link between the data identifying the people and the data concerning them.

[23] See Article 5.1 (e) of the [GDPR], unless there is another legal obligation calling for longer storage periods).

The storage durations, their justification and purge mechanisms can be presented in the table below.

Data types	Storage duration	Justification of the storage duration	Erasure mechanism at the end of the storage duration
Common data			
Archived data			
Functional traces			
Technical logs			

2.2 Controls protecting data subjects' rights

2.2.1 Information for the data subjects (fair and transparent processing)[24]

If the processing benefits from an exemption from the right to information, as provided for in Articles 12, 13 & 14 of the [GDPR], you will need to justify this below.

Exemption from having to inform the data subjects	Justification

Otherwise, below you will find a list of controls intended to provide information to users (or their parents)[25].

You need to describe how they are implemented (preferably by attaching screenshots and document extracts) on the device, mobile app and personal account, and justify the arrangements for or impossibility of implementing them.

Controls for the right to information	Device	Mobile app	Personal account	Justification
Presentation, when the device is activated, of the terms & conditions for use/confidentiality				
Possibility of accessing the terms & conditions for use/confidentiality after activation				
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, the smartphone/tablet or computer, specifying whether these identifiers are communicated to third parties				
Presentation of the user's rights (consent withdrawal, data erasure, *etc.*)				
Information for the user if the app is likely to run in the background				
Information on the secure data storage method, particularly in the event of sourcing				
Information on protection of access to the device				
Arrangements for contacting the company (identity and contact details) about confidentiality issues				

[24] See Articles 12, 13 & 14 of the [GDPR].

[25] See the CNIL's website: "Editeurs de sites pour enfants : n'oubliez pas vos obligations !" (Publishers of websites for children: remember your obligations!).

Controls for the right to information	Device	Mobile app	Personal account	Justification
Information on the possibility of defining directives concerning the post-mortem fate of data				
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 bodies				

NB: in the event that data are transmitted to third-party bodies in relation 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.

NB[26]: App developers, in collaboration with app stores and operating system and device manufacturers, should present the relevant information in a simple manner, in age specific language adapted to young children – possibly via a sound message.

Recommendation: place an information “*QR Code*" on the device and make the users (or their parents) aware of their responsibility to inform third parties that their data are likely to be collected (e.g. the other children conversing with the device or featured on the shared photos).

2.2.2 Obtaining consent, where applicable: express

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented. The data subject must be able to withdraw his/her consent easily at any time[27].

Where the lawfulness of the processing[28] is based on consent, below you will find a list of controls intended to ensure that users' (or their parents') consent has been obtained[29], that there has been a reminder and confirmation of their consent, and the settings associated with the latter have been maintained.

You will have to describe their implementation on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

[26] See the WP29 opinion 02/2013 on apps on smart devices.

[27] See Articles 7 & 8 of the [GDPR].

[28] Concerning the lawfulness of processing, see chapter 2.1.

[29] See on CNIL website: "Editeurs de sites pour enfants : n’oubliez pas vos obligations !" (Publishers of websites for children: remember your obligations!).

Controls for obtaining consent	Device	Mobile app	Personal account	Justification
Express consent during activation				
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 each 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)				
Where the user changes device, smartphone or computer, reinstalls the mobile app or deletes his/her cookies, the settings associated with his/her consent are maintained				

NB[30]: the GDPR has strengthened the legal basis regarding consent for any direct provision of information society services to minors, and the burden of proof (unambiguous) lies with the data controller or processor.

In practice, the consent of the holder of parental responsibility is required for children under 16 years of age, with Member States able to determine a lower age, as long as this is not below 13 years of age. The data controller must make reasonable efforts to check that the holder of parental responsibility has indeed consented, in view of the technological means available.

NB[31]: When consent can legally be obtained from a minor, and the app is intended to be used by a child or a minor, the data controller should pay attention to the minor's potentially limited understanding of and attention for information about data processing.

App developers, in collaboration with app stores and operating system and device manufacturers, should present the relevant information in a simple manner, in age specific language.

[30] See article 8 of [GDPR].

[31] See the WP29 opinion 02/2013 on apps on smart devices.

2.2.3 Exercising rights of access[32] and to data portability[33]

Where the processing benefits from an exemption from the right of access, as provided for in Articles 15 of the [GDPR], you will need to justify this below.

Exemption from the right of access	Justification	Arrangements for responding to the data subjects

Otherwise, below you will find a list of the controls intended to ensure users' (or their parents') right of access to all personal data concerning them.

You will have to describe their implementation on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

Controls for the right of access	Device	Mobile app	Personal account	Justification
Possibility of accessing all of the user's personal data, via the common interfaces				
Possibility of securely consulting the traces of use associated with the user				
Possibility of downloading an archive of all the personal data associated with the user				

Lastly, where the right to data portability applies to processing pursuant to Article 20 of the [GDPR], you will have to describe its implementation below.

Controls for the right to data portability	Device	Mobile app	Personal account	Justification
Possibility of retrieving, in an easily reusable format, personal data provided by the user, so as to transfer them to another service				

[32] See Article 39 of the [DP-Act] and Article 15 of the [GDPR].

[33] See Article 48 of Act 2016-1321 of 7 October 2016 for a digital Republic and Article 20 of the [GDPR].

2.2.4 Exercising the rights to rectification and erasure[34]

Where the processing benefits from an exemption from the right to rectification and erasure, as provided for by Article 17 of the [GDPR] you will need to justify this below.

Exemption from the rights to rectification and erasure	Justification	Arrangements for responding to the data subjects

Otherwise, below you will find a list of controls intended to ensure the right to rectification or erasure of data of users (or their parents[35]) who request this.

You will have to describe their implementation on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

Controls for the rights to rectification and erasure	Device	Mobile app	Personal account	Justification
Possibility of rectifying personal data				
Possibility of erasing personal data				
Indication of the personal data that will nevertheless be stored (technical requirements, legal obligations, *etc.*)				
Implementing the right to be forgotten for minors				
Clear indications and simple steps for erasing data before scrapping the device				
Advice given about resetting the device before selling it				
Possibility of erasing the data in the event the device is stolen				

NB[36]: 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 its Data Protection Authority (the CNIL in France). 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 at the time of publication or creation of an online account can directly and without the need for an explanation, ask the website to erase data concerning him/her at the earliest possible opportunity.

[34] See Articles 40 & 41 of the [DP-Act] and Articles 16, 17 & 19 of the [GDPR].
[35] See on CNIL website: "Editeurs de sites pour enfants : n'oubliez pas vos obligations !" (Publishers of websites for children: remember your obligations!).
[36] See Act 2016-1321 of 7 October 2016 for a digital Republic amending Article 40 of the [DP-Act], which rounds off the "right to be forgotten" as provided for by Article 17 of the [GDPR].

2.2.5 Exercising the rights to restriction of processing and to object[37]

Where the processing benefits from an exemption from the right to restriction and to object, as provided for by Article 21 of the [GDPR], you will need to justify this below.

Exemption from the rights to restriction and to object	Justification	Arrangements for responding to the data subjects

Otherwise, below you will find a list of controls intended to ensure the right to object and to restriction either concerning the different purposes or the whole of a processing operation.

You will have to describe their implementation on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

Controls for the rights to restriction and to object	Device	Mobile app	Personal account	Justification
Existence of "Privacy" settings				
Invitation to change the default settings				
"Privacy" settings accessible when activating the device				
"Privacy" settings accessible after activating the device				
Existence of a parental control system for children under 13 years of age				
Existence of a system allowing the user to ask for the processing to be restricted				
Existence of technical means for the data controller to lock access to and use of the data subject to the restriction				
Possibility of deactivating some of the device's features (microphone, Web browser, *etc.*)				
Existence of alternative apps for accessing the device				
Possibility of objecting to the mobile app running in the background				
Compliance in terms of tracking (cookies, advertising, *etc.*)				
Exclusion of children under 13 years of age from automated profiling				
Effective exclusion of processing the user's data in the event consent is withdrawn				

[37] See Articles 18 & 21 of the [GDPR].

Note: 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.

2.2.6 Processors: identified and governed by a contract[38]

A processing contract must be signed with each processor, setting out all of the aspects stipulated in Art. 28 of the [GDPR]: duration, scope, purpose, documented processing instructions, prior authorization where a processor is engaged, provision of any documentation providing evidence of compliance with the [GDPR], prompt notification of any data breach, *etc.*

Below you will find a table for setting out in detail the contracts for each of the processors.

Processor's name	Purpose	Scope	Contract reference	Compliance with Art.28

2.2.7 Transfers: compliance with the obligations bearing on transfer of data outside the European Union[39]

Below you will find a table for setting out in detail the geographic storage location of the device, mobile app and personal account data in the cloud.

Depending on the country in question, you will have to justify the choice of remote hosting and indicate the legal supervision arrangements implemented in order to ensure adequate protection of the data subject to a cross-border transfer.

Data storage location	France	European Union	Country recognized as providing adequate protection by the EU	Other country	Justification and supervision (standard contractual clauses, internal corporate regulations)
Device data					
Mobile app data					
Personal account data					

[38] See article 28 of [GDPR].

[39] See Articles 44 to 50 of the [GDPR].

2.3 Assessment of compliance with the fundamental principles

Below you will find a table for summarizing, for each point concerning compliance with the legal requirements, the way in which it is applied in the processing.

The last two columns are for use by the assessor:

→Acceptable/can be improved on?

The assessor must estimate whether the controls allow compliance with the fundamental principles.

→Corrective controls:

Where applicable, he shall indicate any additional controls that would prove necessary.

Controls guaranteeing the proportionality and necessity of the processing	Justification	Acceptable/can be improved on?	Corrective controls
Purposes: specified, explicit and legitimate			
Basis: lawfulness of processing, prohibition of misuse			
Data minimization: adequate, relevant and limited			
Quality of data: accurate and kept up-to-date			
Storage durations: limited			
Controls to protect the rights of data subjects	**Justification**	**Acceptable/can be improved on?**	**Corrective controls**
Information for the data subjects (fair and transparent processing)			
Obtaining consent			
Exercising the rights of access and to data portability			
Exercising the rights to rectification and erasure			
Exercising the rights to restriction of processing and to object			
Processors: identified and governed by a contract			
Transfers: compliance with the obligations bearing on transfer of data outside the European Union			

3 Study of data security risks[40]

A risk is a hypothetical scenario that describes a feared event and all the threats that allow this to occur. More specifically, it describes:

- ❑ how risk sources (e.g.: an employee bribed by a competitor)
- ❑ could exploit the vulnerabilities of supporting assets (e.g.: the file management system that allows the manipulation of data)
- ❑ in a context of threats (e.g.: misuse by sending emails)
- ❑ and allow feared events to occur (e.g.: illegitimate access to personal data)
- ❑ on personal data (e.g.: customer file)
- ❑ thus generating impacts on the privacy of data subjects (e.g.: unwanted solicitations, feelings of invasion of privacy, personal or professional problems).

3.1 Assessment of existing or planned controls

Generally performed by the prime contractor[41], then assessed by a person in charge of "Data security" aspects[42].

Objective: gain a good understanding of the controls that contribute to security.

- ❑ Identify or determine the **existing or planned controls** (already undertaken), which can take three different forms:
  1. **controls bearing specifically on the data being processed**: encryption, anonymization, partitioning, access control, traceability, *etc*.;
  2. **general security controls regarding the system in which the processing is carried out**: operating security, backups, hardware security, *etc*.;
  3. **organizational controls (governance)**: policy, project management, personnel management, management of incidents and breaches, relations with third parties, *etc*.
- ❑ Check that improving each control and its description, pursuant to best security practice, is either not necessary or not possible.
- ❑ Where applicable, review their description or propose additional controls.

Notes: The security control categories below correspond to the CNIL's recommended good practices[43].

You will also need to take account of the sector-specific standards applicable to your processing[44] (general security policy, PIA Framework, code of conduct, *etc*.).

Note: In Para. 3.1.4 below, you will find a table for summarizing the implementation of all these controls and for recording their assessment and any corrective controls.

[40] See article 32 of [GDPR].
[41] This may be a delegate, representative or processor.
[42] Chief information security officer or other.
[43] See the "Guide on security of personal data" by the CNIL.
[44] See Article 35 (8) of the [GDPR].

3.1.1 Controls bearing specifically on the data being processed

Encryption

*Describe here the **means implemented for ensuring the confidentiality of data** stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.).*

Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing.

Notes: think about Wi-Fi security (encryption, Wi-Fi password storage).

Think about securing the certificates stored on the device or smartphone, used for authenticating and encrypting connections.

Anonymization

Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose.

Note: remember to clearly distinguish between anonymous and pseudonymous data.

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

Indicate here if processing partitioning is planned, and how this is carried out.

Logical access control

*Indicate here how **users' profiles** are defined and attributed.*

*Specify the **authentication** means implemented*[45].

*Where applicable, specify the rules applicable to **passwords** (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.).*

Notes: think about the security of the user's password, whether on the device, smartphone or in the cloud. Passwords must be stored properly hashed by a robust algorithm with a salt applied beforehand.

Think about protecting access to the app on the smartphone with a specific password.

Think about securing peering between the device, mobile app and personal account.

Think about protecting the data, including metadata (including Exif) and technical traces in the event of direct access via physical connection to the device or smartphone.

[45] See the CNIL deliberation no. 017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords.

Traceability (logging)

*Indicate here whether **events are logged** and how long these traces are stored for.*

Integrity monitoring

Where applicable, indicate here whether mechanisms are implemented for integrity monitoring of stored data, which ones and for what purpose.

Specify which integrity control mechanisms are implemented on data flows.

Archiving

Where applicable, describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy.

State if data may fall within the scope of public archives.

Paper document security

Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed and exchanged.

3.1.2 General security controls regarding the system in which the processing is carried out

The following controls generally concern the security of the whole body. They can particularly be formally documented in a cybersecurity policy (PSSI) or equivalent.

Operating security

*Describe here how the **software updates** (operating systems, applications, etc.) and application of security patches are carried out.*

Note: think about the possibilities of updating the device.

Managing workstations and clamping down on malicious software

Describe here the controls implemented on workstations (automatic locking, firewall, etc.) and state whether an antivirus software is installed and updated at regular intervals on the workstations.

Website security

Indicate here whether ANSSI's "Recommendations for securing websites" have been implemented.

Backups

Indicate here how backups are managed. Clarify whether they are stored in a safe place.

Maintenance

Describe here how physical maintenance of hardware is managed, and state whether this is contracted out.
Indicate whether the remote maintenance of apps is authorized, and according to what arrangements.
Specify whether defective equipment is managed in a specific manner.

Security of computer channels (networks)

Indicate here the type of network on which the processing is carried out (isolated, private or Internet).
Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.

Monitoring

Indicate here whether real-time monitoring of local network is implemented and with what means.
Indicate whether monitoring of hardware and software configurations is carried out and by what means.

Physical access control

Indicate here how physical access control is carried out regarding the premises accommodating the processing (zoning, escorting of visitors, wearing of passes, locked doors and so on).
Indicate whether there are warning procedures in place in the event of a break-in.

Hardware security

Indicate here the controls bearing on ***the physical security of servers and workstations*** *(secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).*

Avoiding sources of risk

Indicate here whether the implantation area is subject to ***environmental disasters*** *(flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.).*
Specify if ***dangerous products*** *are stored in the same area.*

Protecting against non-human sources of risks

Describe here the means of ***fire*** *prevention, detection and fighting.*
Where applicable, indicate the means of preventing ***water damage****.*
Also specify the means of ***power supply*** *monitoring and relief.*

3.1.3 Organizational controls (governance)

Organization

Indicate if the ***roles and responsibilities for data protection*** *are defined.*
Specify whether a person is responsible for the enforcement of privacy laws and regulations.
Specify whether there is a ***monitoring committee*** *(or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.*

Policy (management of rules)

Indicate whether there is an ***IT charter*** *(or equivalent) on data protection and the correct use of IT resources.*

Risk management

Indicate here whether the privacy risks posed by new treatments on data subjects are assessed, whether or not it is systematic and, if applicable, according to which method.
Specify whether an organization-level mapping of privacy risks is established.

Project management

Indicate here whether device ***tests*** *are performed on non-real/anonymous data.*

Management of incidents and data breaches

Indicate here whether IT ***incidents*** *are subject to a documented and tested management procedure.*

Personnel management

Indicate here what awareness-raising controls are carried out with regard to a new recruit.

Indicate what controls are carried out when persons who have been accessing data leave their job.

Relations with third parties

Indicate here, for ***processors*** *requiring access to data, the security controls and arrangements carried out as regards such access.*

Supervision

Indicate here whether the effectiveness and adequacy of privacy controls are monitored.

3.1.4 Assessment of security controls

Below you will find a table for summarizing how each of the security controls recommended by the CNIL is implemented or for justifying why it is not.

The last two columns are for use by the assessor:

→ Acceptable/can be improved on?

The assessor must determine whether the controls comply with the CNIL's recommended good practices.

→ Corrective controls:

Where applicable, he shall indicate any additional controls that would prove necessary.

Controls bearing specifically on the data being processed	Implementation or justification why not	Acceptable/can be improved on?	Corrective controls
Encryption			
Anonymization			
Data partitioning (in relation to the rest of the information system)			
Logical access control			
Traceability (logging)			
Integrity monitoring			
Archiving			
Paper document security			
General security controls regarding the system in which the processing is carried out	**Implementation or justification why not**	**Acceptable/can be improved on?**	**Corrective controls**
Operating security			
Managing workstations and clamping down on malicious software			
Website security			
Backups			
Maintenance			
Security of computer channels (networks)			
Monitoring			
Physical access control			
Hardware security			
Avoiding sources of risk			
Protecting against non-human sources of risks			

Organizational controls (governance)	Implementation or justification why not	Acceptable/can be improved on?	Corrective controls
Organization			
Policy (management of rules)			
Risk management			
Project management			
Management of incidents and data breaches			
Personnel management			
Relations with third parties			
Supervision			

3.2 Risk assessment: potential privacy breaches

Generally performed by the project owner, then assessed by a person in charge of "Data protection" aspects.

Objective: gain a good understanding of the causes and consequences of risks.

- For each feared event (illegitimate access to personal data[46], unwanted change of personal data[47], and disappearance of personal data[48]) :
  - determine the potential **impacts**[49] on data subjects' privacy if it occurred[50] ;
  - estimate its **severity**, particularly depending on the prejudicial nature of the potential impacts and, where applicable, controls likely to modify them;
  - Identify the **threats**[51] to personal data supporting assets that could lead to this feared event[52] and **the risk sources**[53] that could cause it;
  - estimate its **likelihood**, particularly depending on the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them;
- Determine whether the risks identified in this way[54] can be considered acceptable in view of the existing or planned controls (already undertaken).
- If not, propose additional controls and re-assess the level of each of the risks in view of the latter, so as to determine the residual risks[55].

NB: since the existing or planned controls (already undertaken) are taken on board in the risk assessment, before moving on to Part 3.2, the controls identified in Para. 2 (legal) and Para. 3.1 (security) must first have been assessed to ensure that their list is exhaustive and properly reflects the way things really are.

NB: any corrective controls suggested by the assessor in Paras 2.3 and 3.1.4 must be taken into account during the residual risk calculation in Paras 3.2.1, 3.2.2 and 3.2.3, at the same time as the corrective controls specific to each of the risks.

All of the corrective controls will be set out in the action plan in Para. 4.1.

[46] They are known to unauthorised persons (data confidentiality breach).
[47] They are altered or changed (breach of personal data integrity).
[48] They are not or no longer available (breach of personal data availability).
[49] See Appendix 3 – Severity scale and examples of impacts.
[50] Answer the question "What do we fear might happen to data subjects?"
[51] See Appendix 4 – Likelihood scale and examples of threats.
[52] Answer the question "How might this happen?"
[53] See Appendix 2 – Risk sources.
[54] A risk is based upon a feared event and all threats that would make it possible.
[55] Risks that remain after the controls have been implemented.

3.2.1 Illegitimate access to personal data

Assessment of the risk

Below you will find a table for noting down the result of the analysis of this risk.

To show how to use it, it has been completed with the data from our example of a fictional toy.

Risk	Main risk sources[56]	Main threats[57]	Main potential impacts[58]	Main controls reducing the severity and likelihood[59]	Severity[60]	Likelihood[61]
Illegitimate access to personal data	Rogue acquaintances Rogue neighbor Rogue employee Authorized third-party company Hacker targeting a user or one of the companies	Data theft/consultation on the server Account theft (via a smartphone) Recovery of a scrapped device	Consequences of the disclosure of potentially sensitive information (discrimination, threats, attacks, loss of employment, loss of access to services, *etc.*) Phishing Targeted advertising	Minimization Storage durations Logical access control Stream encryption (SSL) Hardware authentication Private cloud Logical access control Employee clearance Access logging Log audits Notification of data subject violations and recommendation of suitable preventive controls	Significant	Maximum

Describe here a few representative scenarios of the risk of illegitimate data access, by spelling out the sources, threats and impacts.

Below you will find an illustration based on our example of a fictional toy:

Data could be stolen by an employee with a profit motive or malicious intent, consulted by family or friends taking over the account via the smartphone, or retrieved on a scrapped device by neighbors or a hacker with a view to characterizing a situation bearing on the data subjects' private life.

[56] Relevant sources for this risk, among those identified in the context of the processing (see Appendix 2 – Risk sources).
[57] See Appendix 4 – Likelihood scale and examples of threats.
[58] See Appendix 3 – Severity scale and examples of impacts.
[59] Controls among those identified in Para. 2 (legal) and Para. 3.1 (security).
[60] See Appendix 3 – Severity scale and examples of impacts.
[61] See Appendix 4 – Likelihood scale and examples of threats.

Assessment of residual risks

→ Acceptable/can be improved on?

The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.

→ Corrective controls:

Where applicable, he shall indicate here any additional controls that would prove necessary.

→ Residual risks:

The assessor will indicate here the residual risk for the processing once the aforementioned additional controls have been implemented, by determining the severity and likelihood in view of these controls.

Severity*:* ***Likelihood****:*

NB: an additional control carried out to deal with one of the risks can also have a positive or negative effect on the other risks.

Below you will find an illustration based on our example of a fictional toy:

→ Can be improved on*:*

The planned controls do not sufficiently reduce this risk for it to be deemed acceptable.

→ Corrective controls*:*

- carry out encryption of the data stored in the base;
- inform the user of the good practices to follow when scrapping the device;
- supply a charter on using IT equipment and a confidentiality undertaking for employees.

→ Residual risks:

Data could be consulted by family or friends, taking over the account via the smartphone.

Severity*: Significant* ***Likelihood****: Negligible*

3.2.2 Unwanted change of data

Assessment of the risk

Below you will find a table for noting down the result of the analysis of this risk. To show how to use it, it has been completed with the data from our example of a fictional toy.

Risks	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Unwanted change of data	Negligent or rogue user /family member /friend Rogue neighbor Negligent or rogue employee Hacker targeting one of the companies	Alteration of data on the server	Identity theft Deterioration in the service quality	Backup of the cloud server Stream encryption (SSL) Hardware authentication Private cloud Logical access control Employee clearance Access logging Log audits Notification of data subject violations and recommendation of suitable preventive controls	Limited	Limited

Describe here a few representative scenarios of the risk of an unwanted change of data by spelling out the sources, threats and impacts.

Assessment of residual risks

→ *Acceptable/can be improved on?*

The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.

→ *Corrective controls:*

Where applicable, he shall indicate here any additional controls that would prove necessary.

→ *Residual risks:*

The assessor will indicate here the residual risk for the processing once the aforementioned additional controls have been implemented, by determining the severity and likelihood in view of these controls.

Severity: ***Likelihood***:

3.2.3 Disappearance of data

Assessment of the risk

Below you will find a table for noting down the result of the analysis of this risk. To show how to use it, it has been completed with the data from our example of a fictional toy.

Risks	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Disappearance of data	Negligent or rogue user /family member /friend Negligent or rogue employee Hacker targeting a user or one of the companies Damage at one of the companies	Erasure of data (via the app or server) Deterioration of servers Physical damage to the device	Need to recreate a user account Loss of history and personal service settings Deterioration in the service quality	Backup of the cloud server Private cloud Physical protection of the cloud servers Maintenance Temporary on-premises data retention Logical access control Employee clearance Strong authentication of employees Access logging Warranty for the device	Limited	Limited

Describe here a few representative scenarios of the risk of data disappearing, by spelling out the sources, threats and impacts.

Assessment of residual risks

→Acceptable/can be improved on?

The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.

→Corrective controls:

Where applicable, he shall indicate here any additional controls that would prove necessary.

→Residual risks:

The assessor will indicate here the residual risk for the processing once the aforementioned additional controls have been implemented, by determining the severity and likelihood in view of these controls.

***Severity**:* ***Likelihood**:*

4 Validation of the PIA

Generally performed by the controller, with the help of a person in charge of "Data Protection" aspects.

Objective: decide whether or not to accept the PIA in light of the study's findings.

4.1 Preparation of the material required for validation

- ❑ Consolidate and present the study's findings:
  1. prepare a visual presentation of the **controls selected to ensure compliance with the fundamental principles,** depending on their compliance with the [GDPR] (e.g.: conditional on improvement or considered compliant);
  2. prepare a visual presentation of the **controls selected to contribute to data security**, depending on their compliance with best security practice (e.g.: conditional on improvement or considered compliant);
  3. visually map the **risks** (initial and residual where applicable[62]) depending on their severity and likelihood;
  4. draw up an **action plan** based on the additional controls identified during the previous steps: for each control, determine at least the person responsible for its implementation, its cost (financial or in terms of workload) and estimated timeframe.

- ❑ Formally document the consideration of stakeholders:
  1. the **advice of the person in charge of "Data Protection" aspects**[63];
  2. the **view of data subjects or their representatives**[64].

Note: The spaces for noting down the assessment of controls and risks are inserted directly into the previous parts, as near to the aspects to be assessed as possible.

All of the parts must be assessed before deciding on whether the PIA can be validated or not.

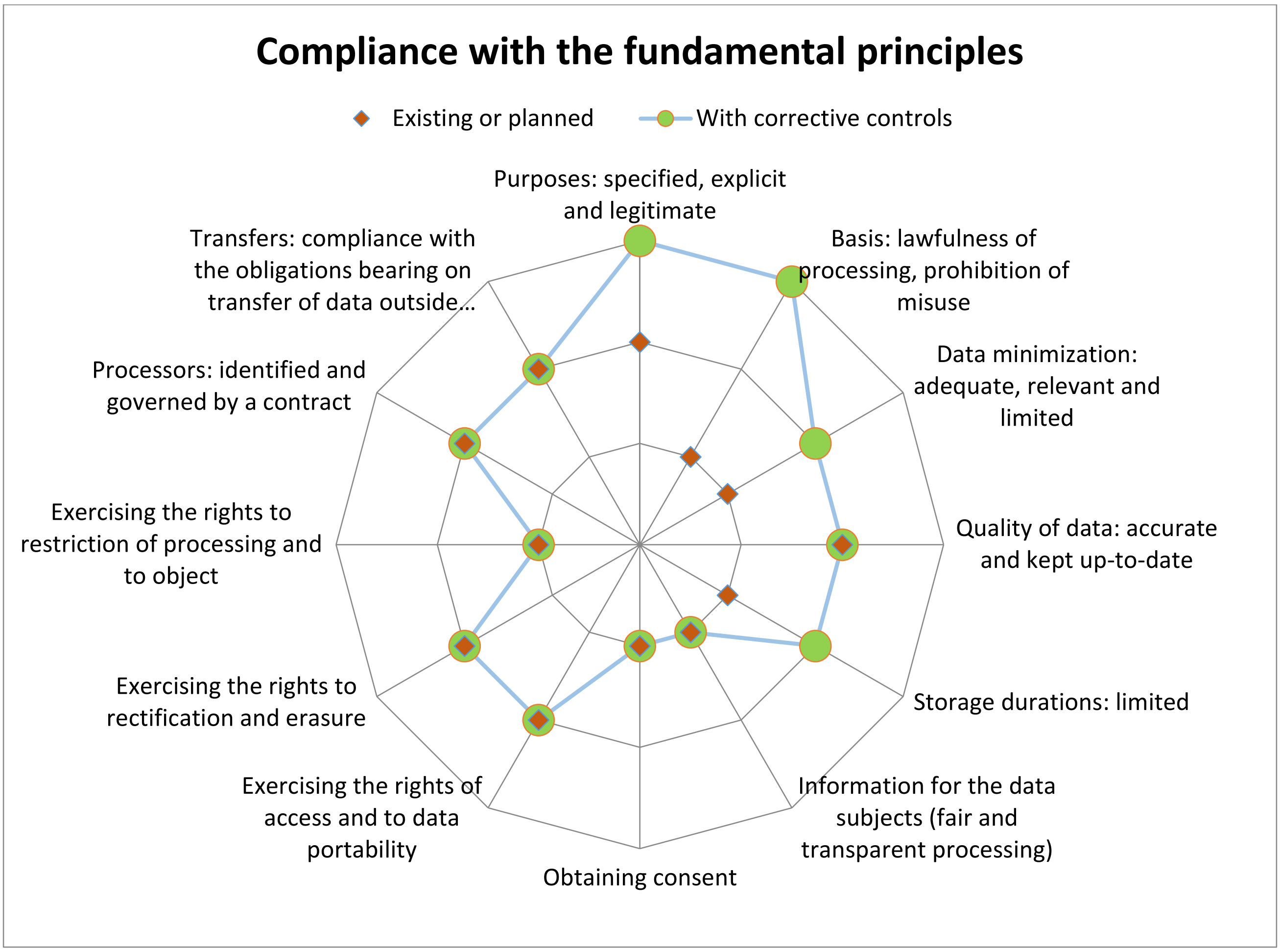
[62] Risks that remain after the controls have been implemented.
[63] See Article 35 (2) of the [GDPR]
[64] See Article 35 (9) of the [GDPR]

4.1.1 Mapping of compliance with the fundamental principles

Below you will find a graph illustrating the controls bearing on compliance with the fundamental principles, with a conformity value attributed to each on the basis of its assessment in Para. 2.3.

To show how to use it, it has been completed with the data from our example of a fictional toy.

If the additional controls are implemented correctly, compliance with the fundamental principles could be illustrated as follows:



Graph scale:

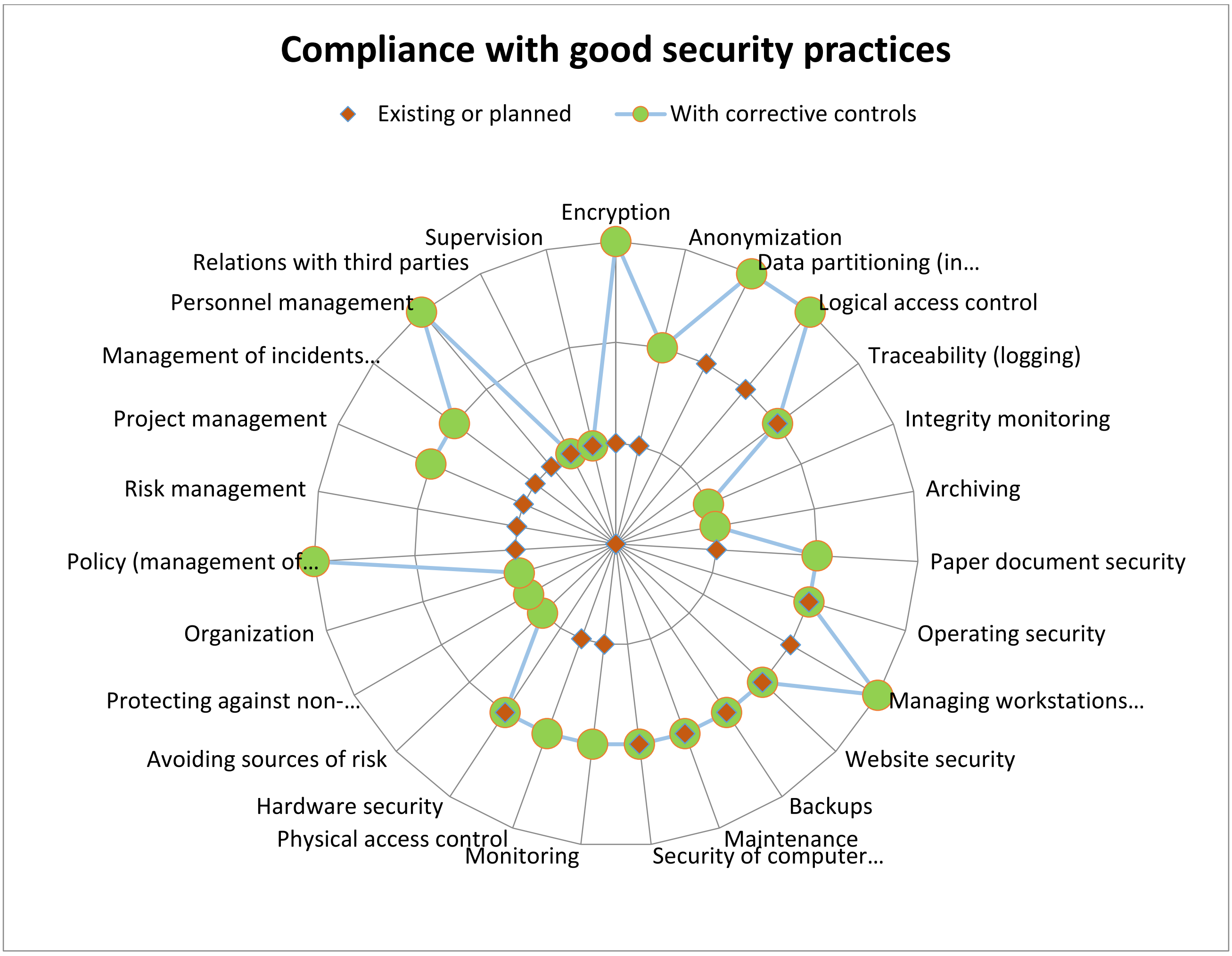
0. Non applicable
1. Can be improved on
2. Acceptable
3. Good practices

4.1.2 Mapping of compliance with good security practices

Below you will find a graph illustrating the good security practices, with a conformity value attributed to each on the basis of its assessment in Para. 3.1.4.

To show how to use it, it has been completed with the data from our example of a fictional toy.

If the additional controls are implemented correctly, compliance with the good security practices could be illustrated as follows:



Graph scale:

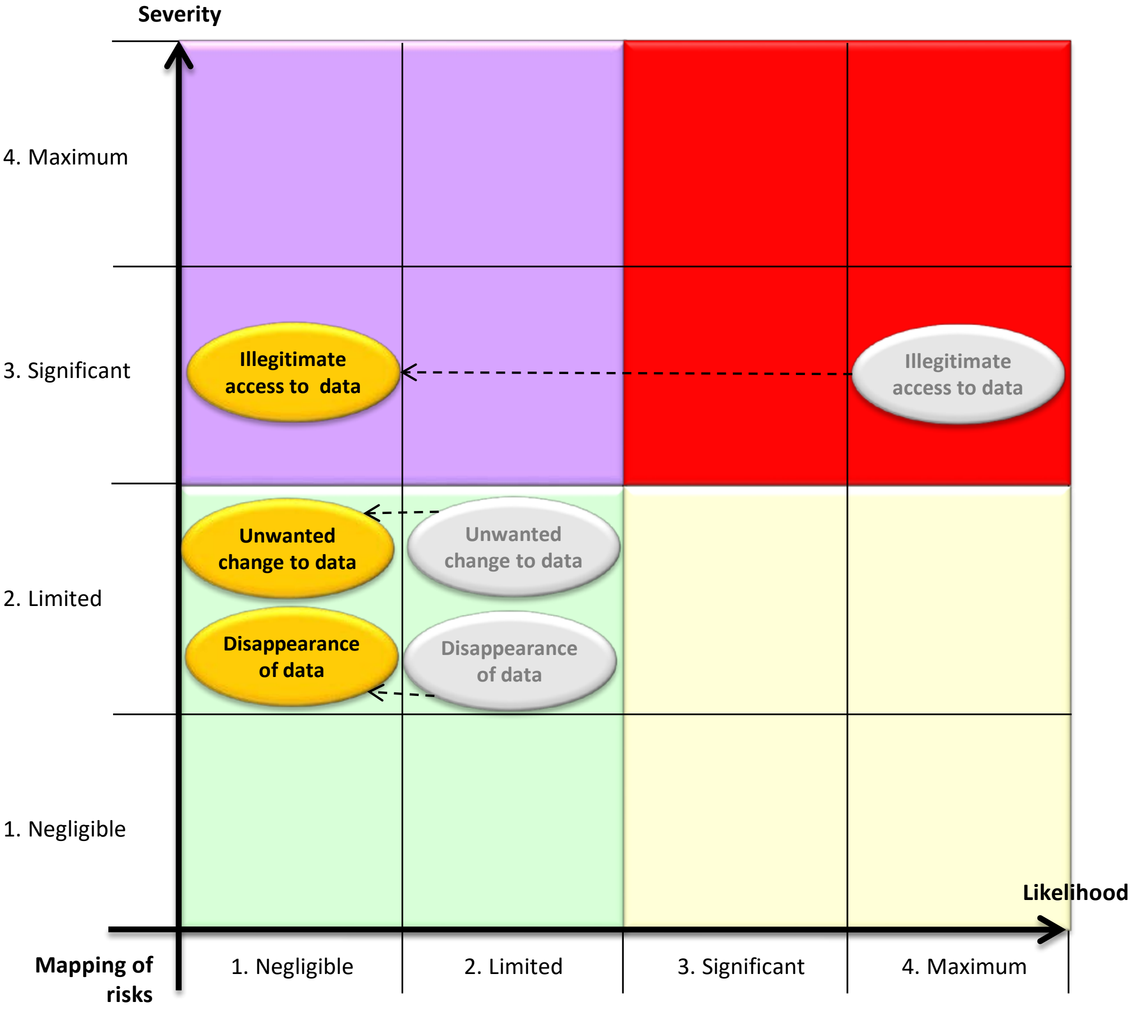
0. Non applicable
1. Can be improved on
2. Acceptable
3. Good practices

4.1.3 Mapping of risks

Below you will find a graph illustrating the good security practices, with a conformity value attributed to each on the basis of its assessment in Para. 4.1.

To show how to use it, it has been completed with the data from our example of a fictional toy.

If the additional controls are implemented correctly, the residual risks should be as follows:



4.1.4 Action plan: details on the planned additional controls

Below you will find a table to group together all the corrective controls suggested by the assessor in Paras 2.3, 3.1.4, 3.2.1, 3.2.2 and 3.2.3, and thus draw up an action plan setting out, for each action, its manager, deadline, difficulty, cost and progress (see Appendix 5 – Scales for the action plan).

To show how to use it, it has been completed with the data from our example of a fictional toy.

Additional controls requested	Manager	Deadline	Difficulty	Cost	Progress
Inform the user of the good practices to follow when scrapping the hardware	Customer service and CISO	Month	Low	Nil	Not started
Supply a charter on using IT equipment for employees	Legal service and CISO	Month	Low	Nil	In progress
Set up a confidentiality undertaking for employees	Legal service and CISO	Month	Low	Nil	Not started
Carry out encryption of the data stored in the base	Prime contractor and CISO	Quarter	Moderate	Moderate	Not started

NB: all of the controls specified under the action plan will have to be formally documented, set up and monitored at regular intervals and subject to continuous improvement.

4.1.5 Advice of the person in charge of "Data Protection" aspects [65]

Below you will find a space for noting down the general view of the person in charge of "Data Protection" aspects, prior to validation.

Note: this view may be against the processing being implemented, without restricting the decision of the data controller for all that.

On dd/mm/yyyy, the Data Protection Officer of the company X issued the following opinion concerning the compliance of the processing and PIA study carried out:

[Signature]

[65] See Article 35 (2) of the [GDPR].

4.1.6 View of data subjects or their representatives[66]

Below you will find a space for noting down the view of the data subjects or their representatives on the intended processing.

NB[67]: the data controller must seek the views of the data subjects or their representatives, where applicable.

These views may be gathered by diverse means, depending on the context (internal or external study on the processing methods and purpose, question for the attention of staff representatives or trade unions, survey among future customers of the data processor).

Where the data controller decides to go against the views of the data subjects, he must note down the justification for this decision.

Where the data controller considers that gathering the views of the data subjects is not relevant, he must also note down the justification thereof.

The data subjects [were/were not] consulted [and expressed the following view on the compliance of the processing in light of the study performed]:

Justification of the data controller's decision:

[66] See Article 35 (9) of the [GDPR].

[67] See the WP29 Guidelines on PIAs (in English).

4.2 Formal validation of the PIA

- Decide on whether the selected controls, residual risks and action plan are acceptable, with justifications, in view of the previously identified stakes and views of the stakeholders. In this way, the PIA may be:
    - validated;
    - conditional on improvement (explain in what way);
    - refused (along with the processing under consideration).

- Where necessary, repeat the previous steps so that the PIA can be validated[68].

Note: this decision does not prejudge the compliance assessment which may be carried out, where applicable, by the Data Protection Authority (the CNIL in France), as part of preliminary formalities or checks for example.

Below you will find a PIA formal validation example, illustrated using the information from our example of a fictional toy.

On dd/mm/yyyy, the Managing Director of the company X validates the PIA for the processing of the connected toy, in light of the study carried out, in his capacity as data controller.

The purposes of the processing are to provide interactivity to the child, through the possibility of dialogue with the toy (questions/answers in natural language by voice recognition), enable the child to communicate online (send voice messages, texts and photos) with his/her friends and/or parents and feed information back to the parents (surveillance device).

The controls planned for complying with the fundamental principles underpinning privacy protection and for addressing the risks to the privacy of data subjects have indeed been deemed acceptable in light of these stakes. The implementation of additional controls will nevertheless have to be demonstrated, as will continuous improvement of the PIA.

[Signature]

[68] See, in particular, Appendix 6 – Typology of objectives to address the risks.

Appendices

1. Data minimization controls

Minimization controls	Description
Filtering and removal	When data are being imported, different types of metadata (such as EXIF data attached with an image file) can unintentionally be collected. Such metadata must be identified and eliminated if they are unnecessary for the purposes specified.
Reducing sensitivity via conversion	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.
Reducing the identifying nature of data	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.
Reducing data accumulation	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.
Restricting data access	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 shadow files which are produced during the data processing must also be protected.

2. Risk sources

By way of an example, the table below describes the risk sources and their capabilities, which are relevant in the context of our example of our fictional toy.

Types of risk sources	Relevant risk sources	Description of capabilities	Description of motives	Decision
Internal human sources acting accidentally or intentionally	**Negligent or rogue employee**	Proximity of the system, skills, privileges and available time are potentially high, possible lack of training and awareness	Clumsiness, error, negligence Revenge, desire to whistleblow, malicious intent Profit motive, spying,	Adopted
	Negligent or rogue user /family member /friend	Direct access to the device and app	Clumsiness, error, negligence Game, malicious intent Revenge, spying	Adopted
External human sources acting intentionally	**Rogue neighbor**	Physical proximity making it possible to hack into the device's data	Game, disruption, malicious intent Revenge, spying	Adopted
	Hacker targeting a user	Knowledge of the user and some of the information concerning him/her	Game, disruption, malicious intent Revenge, spying	Adopted
	Hacker targeting one of the companies	Knowledge of the companies that can undermine their image	Revenge, desire to whistleblow, malicious intent Profit motive, spying	Adopted
	Authorized third-party company	Privileged access can be used to illegitimately access information	Profit motive, desire to get hold of a large amount of data and to use them	Adopted
External human sources acting accidentally	**Naive neighbor**	Physical proximity making it possible to emit on the device's communication channel	Ignorance	Not adopted
Non-human sources	**Incident or damage at the user's** (power cut, fire, flood, *etc.*)	Diverse		Not adopted
	Damage at one of the companies (power cut, fire, flood, *etc.*)	Diverse		Adopted

3. Severity scale and examples of impacts

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[69]	Examples of material impacts[70]	Examples of moral impacts[71]
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 (e.g.: 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

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

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[69]	Examples of material impacts[70]	Examples of moral impacts[71]
			Processing of incorrect data creating for example account 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)

4. Likelihood scale and examples of threats

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 action of risk sources on the supporting assets constitutes a threat. The supporting assets can be:

- used inappropriately: supporting assets are used outside or even diverted from their intended context of use without being altered or damaged;
- observed: supporting assets are observed or spied upon without being damaged;
- overloaded: the limits of operation of supporting assets are exceeded, supporting assets are overloaded, over-exploited or used under conditions not permitting them to function properly;
- damaged: supporting assets are partially or completely damaged;
- altered: supporting assets are transformed;
- lost: supporting assets are lost, stolen, sold or given away, so it is no longer possible to exercise property rights.

The generic threats that follow are designed to be exhaustive, independent and applied to the specific features of privacy protection.

Threats that can lead to an illegitimate access to personal data

Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
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 in other ways than the intended purpose, disproportion between hardware capacities and the required capacities (e.g. hard drive of several TB to store a few GB of data)
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
Hardware	Altered	Tracking by a hardware-based key logger, removal of hardware	Allows components (boards, expansion cards) to be added, removed or

Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
		components; connection of devices (such as: USB flash drives) to launch an operating system or retrieve data	substituted via connectors (ports, slots); allows components to be disabled (USB port)
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)
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
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
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
Computer channels	Observed	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network	Permeable (generation of emanations that may or may not be compromising); allows interpretable data to be observed
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)
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)
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
Paper documents	Observed	Reading, photocopying, photographing	Allows interpretable data to be seen
Paper documents	Lost	Theft of files from offices; theft of mail from mailboxes; retrieval of discarded documents	Portable
Paper transmission channels	Observed	Reading of signature books in circulation; reproduction of documents in transit	Observable

Threats that can lead to an unwanted modification of personal data

Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
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)
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
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
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)
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
People	Manipulated	Influence (rumor, disinformation)	Easily influenced (naive, gullible, obtuse)
Paper documents	Altered	Changes to figures in a file; replacement of an original by a forgery	Falsifiable (paper documents with editable content)
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

Threats that can lead to a disappearance of personal data

Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
Hardware	Used inappropriately	Storage of personal files; personal use	Usable in other ways than the intended purpose
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 suited to the conditions of use; constant electricity supply required for operation; sensitive to voltage variations
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)
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)
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)
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
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
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
Software	Damaged	Erasure of a running executable or source codes, virus, logic bomb	Possibility of erasing or deleting programs; sole copy; complex in terms of use (not very user-friendly, few explanations)
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)
Computer channels	Overloaded	Misuse of bandwidth; unauthorized downloading; loss of Internet connection	Non-scalable transmission capacities (insufficient bandwidth; limited amount of telephone numbers)

Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
Computer channels	Damaged	Cut wiring, poor Wi-Fi reception, corrosion of cables	Alterable (fragile, breakable, poor cable structure, bare cables, disproportionate sheath), sole
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)
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
People	Damaged	Occupational accident; occupational disease; other injury or disease; death; neurological, psychological or psychiatric ailment	Physical, psychological or mental limits
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
Paper documents	Used inappropriately	Gradual erasure over time; deliberate 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)
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
Paper documents	Lost	Theft of documents; loss of files during a move; disposal	Portable
Paper transmission channels	Overloaded	Mail overload; overburdened validation process	Existence of quantitative or qualitative limits
Paper transmission channels	Damaged	End of workflow following a reorganization; mail delivery halted by a strike	Unstable, sole
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)
Paper transmission channels	Lost	Elimination of a process following a reorganization; loss of a document delivery company, vacancy	Unrecognized need

5. Scales for the action plan

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

Criterion	Level 1	Level 2	Level 3
Difficulty	Low	Moderate	High
Financial cost	Nil	Moderate	Significant
Deadline	Year	Quarter	Month
Progress	Not started	In progress	Completed

6. Typology of objectives to address the risks

Objectives can be set depending on the risk level, for example:

1. Risks with a high severity and likelihood[72]: these risks must absolutely be avoided or reduced by implementing security controls that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that they are addressed by independent controls of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event);
2. Risks with a high severity but a low likelihood[73]: these risks must be avoided or reduced by implementing security controls that reduce both their severity and their likelihood. Emphasis must be placed on preventive controls. These risks can be taken, but only if it is shown that it is not possible to reduce their severity and if their likelihood is negligible;
3. Risks with a low severity but a high likelihood: these risks must be reduced by implementing security controls that reduce their likelihood. Emphasis must be placed on recovery controls. These risks can be taken, but only if it is shown that it is not possible to reduce their likelihood and if their severity is negligible;
4. Risks with a low severity and low likelihood: it should be possible to take these risks, especially since the processing of other risks should also lead to these being addressed.

Notes: The risks can generally be reduced, transferred or retained. However, some risks cannot be taken, especially when sensitive data are processed or when the damages that data subjects may sustain are very significant. In such cases it may be necessary to avoid them, for example by not implementing all or part of the processing.

[72] Levels 3. Significant and 4. Maximum.

[73] Levels 1. Negligible and 2. Limited.