Privacy Impact Assessment (PIA)

TEMPLATES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

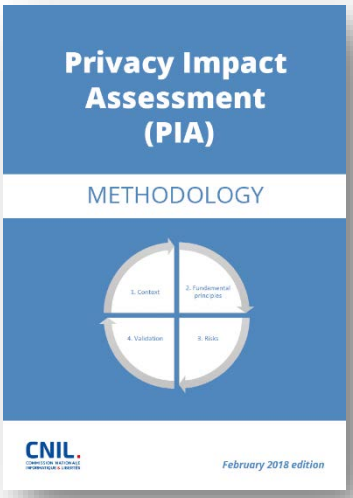
February 2018 edition

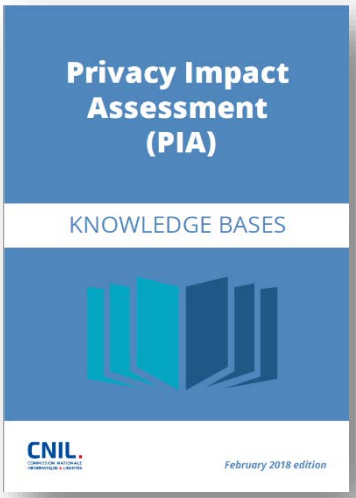
Contents

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Foreword

The methodology of the French Data Protection Authority (CNIL) comprises three guides: one setting out the approach, a second containing facts that could be used for 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's website:

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

Writing conventions for all of these documents:

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

Attention: the templates presented in this guide constitute an aid to the implementation of the approach. It is entirely possible and even desirable to adapt them to each particular context.

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

1 Study of the context: templates

1.1 Overview of the processing

Description of the processing under consideration

Description of the processing[1]	
Processing purposes	
Processing stakes	
Controller	
Processor(s)	

Sector-specific standards applicable to the processing[2]

Standards applicable to the processing	Consideration

1.2 Data, processes and supporting assets

Data description, recipients and storage durations

Data types	Recipients	Storage duration

Description of the processes and supporting assets

[insert a diagram of data flows and a detailed description of the processes carried out]

Processes	Detailed description of the process	Data supporting assets

[1] Its nature, scope, context, *etc.*
[2] See Article 35 (8) of the [GDPR].

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

2 Study of the fundamental principles: templates

2.1 Assessment of the controls guaranteeing the proportionality and necessity of the processing

Explanation and justification of purposes

Purposes	Legitimacy

Explanation and justification of lawfulness

Lawfulness criteria	Applicable	Justification
The data subject has given consent[3] 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[4]		

[3] With regard to obtaining the data subject's consent and informing the latter, see Chapter 2.2.
[4] This point shall not apply to processing carried out by public authorities in the performance of their tasks.

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Explanation and justification of data minimization

Details about the data processed	Data categories	Justification of the need and relevance of the data	Minimization controls

Explanation and justification of data quality

Data quality controls	Justification

Explanation and justification of storage durations

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			

Assessment of the controls

Controls guaranteeing the proportionality and necessity of the processing	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		
Data quality: accurate and kept up-to-date		
Storage durations: limited		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

2.2 Assessment of controls protecting data subjects' rights

Determination and description of the controls for information for the data subjects

If the processing benefits from an exemption from the right to information, as provided for in Article 32 of the [DP-Act] and Articles 12, 13 & 14 of the [GDPR]:

Exemption from having to inform the data subjects	Justification

Otherwise:

Controls for the right to information	Implementation	Implementation justification or justification why not
Presentation of the terms & conditions for use/confidentiality		
Possibility of accessing the terms & conditions for use/confidentiality		
Legible and easy-to-understand terms		
Existence of clauses specific to the device		
Detailed presentation of the data processing purposes (specified objectives, data matching where applicable, *etc.*)		
Detailed presentation of the personal data collected		
Presentation of any access to the identifiers of the device, the smartphone/tablet or computer, by specifying whether these identifiers are communicated to third parties		
Presentation of the user's rights (consent withdrawal, data erasure, *etc.*)		
Information on the secure data storage method, particularly in the event of sourcing		
Arrangements for contacting the company (identity and contact details) about confidentiality issues		
Where applicable, information for the user on any change concerning the data collected, the purposes and confidentiality clauses		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Controls for the right to information	Implementation	Implementation justification or justification why not
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		

Determination and description of the controls for obtaining consent[5]

Controls for obtaining consent	Implementation	Implementation justification or justification why not
Express consent during registration		
Consent segmented per data category or processing type		
Express consent prior to sharing data with other users		
Consent presented in an intelligible and easily accessible form, using clear and plain language adapted to the target user (particularly for children)		
Obtaining parents' consent for minors under 13 years of age		
For a new user, consent must once again be obtained		
After a long period without use, the user must be asked to confirm his/her consent		
Where the user has consented to the processing of special data (e.g. his/her location), the interface clearly indicates that said processing takes place (icon, light)		
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		

Determination and description of the controls for the rights of access and to data portability

[5] Where processing lawfulness is based on consent.

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Where the processing benefits from an exemption from the right of access, as provided for in Articles 39 & 41 of the [DP-Act] and Articles 15 of the [GDPR]:

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

Otherwise:

Controls for the right of access	Internal data	External data	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]:

Controls for the right to data portability	Internal data	External data	Justification
Possibility of retrieving, in an easily reusable format, personal data provided by the user, so as to transfer them to another service			

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Determination and description of the controls for the rights to rectification and erasure

Where the processing benefits from an exemption from the right to rectification and erasure, as provided for by Article 41 of the [DP-Act] and Article 17 of the [GDPR]:

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

Otherwise:

Controls for the rights to rectification and erasure	Internal data	External data	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			

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Determination and description of the controls for the rights to restriction of processing and to object

Where the processing benefits from an exemption from the right to restriction and to object, as provided for by Article 38 of the [DP-Act] or Article 21 of the [GDPR]:

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

Otherwise:

Controls for the rights to restriction and to object	Internal data	External data	Justification
Existence of "Privacy" settings			
Invitation to change the default settings			
"Privacy" settings accessible during registration			
"Privacy" settings accessible after registration			
Existence of a parental control system for children under 13 years of age			
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			

Determination and description of the controls applicable to processors

Processor's name	Purpose	Scope	Contract reference	Compliance with Art.28[6]

[6] 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 authorisation where a processor is engaged, provision of any documentation providing evidence of compliance with the [GDPR], prompt notification of any data breach, *etc.*

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Determination and description of the controls on transfer of data outside the European Union

Data sets and storage location	France	EU	Country recognized as providing adequate protection by the EU	Other country	Justification and supervision (standard contractual clauses, internal corporate regulations)

Assessment of the controls

Controls to protect the rights of data subjects	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		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

3 Study of data security risks: templates

3.1 Assessment of security controls

Description and assessment of controls implemented for treating the risks related to data security

Controls bearing specifically on the data being processed	Implementation or justification why not	Acceptable/can be improved on?	Corrective controls
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.*]		
Anonymization	[*Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose.*]		
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 whether the users' profiles are defined and attributed.* *Specify the authentication means implemented.* *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.).*]		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Controls bearing specifically on the data being processed	Implementation or justification why not	Acceptable/can be improved on?	Corrective controls
Traceability (logging)	[Indicate here whether events are logged and how long these traces are stored for.]		
Integrity monitoring	[*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	[*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.*]		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Description and assessment of general security controls

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	[*Describe here how the software updates (operating systems, applications, etc.) and application of security corrective controls are carried out.*]		
Clamping down on malicious software	[*State here whether an antivirus software is installed and updated at regular intervals on the workstations.*]		
Managing workstations	[*Describe here the controls implemented on workstations (automatic locking, firewall, etc.).*]		
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).*		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

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
	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 belonging to customers (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*		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

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
	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.]*		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Description and assessment of organizational controls (governance)

Organizational controls (governance)	Implementation or justification why not	Acceptable/can be improved on?	Corrective controls
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*		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Organizational controls (governance)	Implementation or justification why not	Acceptable/can be improved on?	Corrective controls
	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.*]		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

3.2 Risk assessment: potential privacy breaches

Analysis and assessment of risks

Risk	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Illegitimate access to data						
Unwanted change of data						
Disappearance of data						

Assessment of the risks

Risks	Acceptable/can be improved on?	Corrective controls	Residual severity	Residual likelihood
Illegitimate access to data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		
Unwanted change of data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		
Disappearance of data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

4 Validation of the PIA: templates

4.1 Preparation of the material required for validation

Elaboration of the synthesis regarding compliance with [GDPR] of the controls selected to ensure compliance with the fundamental principles

Caption				
Symbol :	●●●	●○○	○●○	○○●
Meaning :	Non applicable	Unsatisfactory	Planned improvement	Acceptable

Controls selected to ensure compliance with the fundamental principles	Assessment
Controls guaranteeing the proportionality and necessity of the processing	
Purpose(s): 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 personal rights of data subjects	
Information for the data subjects (fair and transparent processing)	○○○
Obtaining consent	○○○
Exercising the right of access and right to data portability	○○○
Exercising the rights to rectification and erasure	○○○
Exercising the right to restriction of processing and right to object	○○○
Processors: identified and governed by a contract	○○○
Transfers: compliance with the obligations bearing on transfer of data outside the European Union	○○○

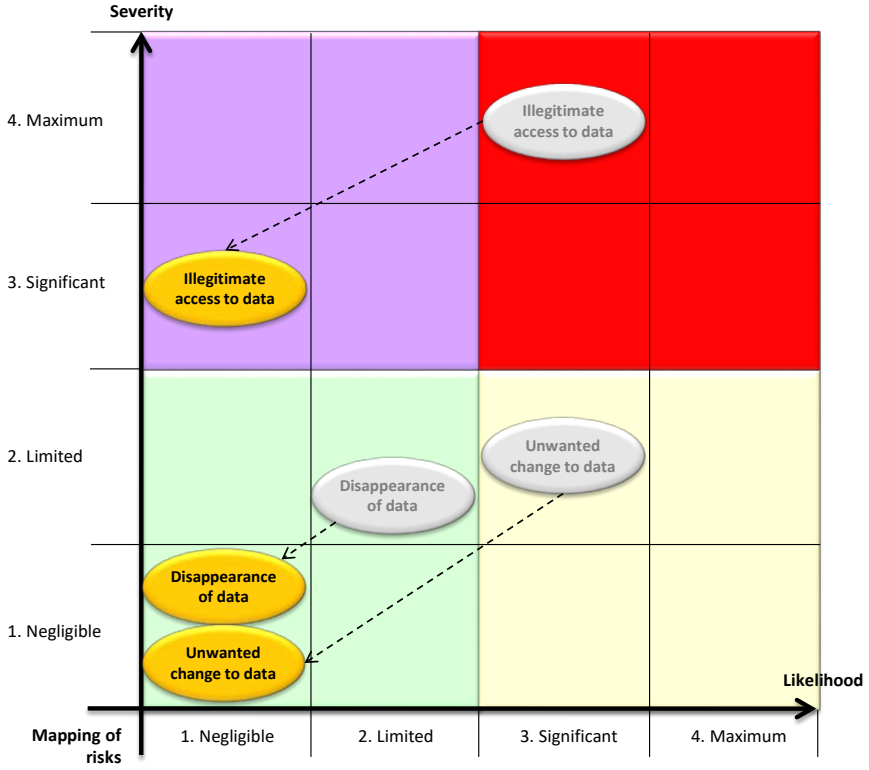
Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Elaboration of the synthesis regarding compliance with good security practices of controls implemented for treating the risks related to data security

Controls implemented for treating the risks related to data security	Assessment
Controls bearing specifically on the data being processed	
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	
Operating security	○○○
Clamping down on malicious software	○○○
Managing workstations	○○○
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)	
Organization	○○○
Policy (management of rules)	○○○
Risk management	○○○
Project management	○○○
Management of incidents and data breaches	○○○
Personnel management	○○○
Relations with third parties	○○○
Supervision	○○○

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Mapping of risks related to data security



Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

Elaboration of action plan

Additional controls requested	Manager	Frequency	Difficulty	Cost	Progress

Documentation of the advice of the person in charge of "Data Protection" aspects[7]

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]

Documentation of the view of data subjects or their representatives[8]

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:

[7] See Article 35 (2) of the [GDPR].
[8] See Article 35 (9) of the [GDPR].

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

4.2 Formal validation of the PIA

Documentation of the validation

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 enable the child to be interactive, 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).

This is because the controls planned for complying with the fundamental principles underpinning privacy protection and for addressing the risks to the privacy of data subjects have 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]

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".