CNIL

Decision No. 2014-017 dated 23 January 2014 adopting a standard for the delivery of privacy seals concerning digital safe boxes

The French data protection authority,

Pursuant to Convention No. 108 of the Council of Europe for the protection of persons with regard to the automated processing of personal data;

Pursuant to directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

Pursuant to Act No. 78-17 dated 6 January 1978 amended (French data protection act), particularly its articles 11, 3 , (c) and13;

Pursuant to decree No. 2005-1309 dated 20 October 2005 for the application of the Act No. 78-17 dated 6 January 1978 relative to the protection of data;

Pursuant to decision No. 2013-175 dated 4 July 2013 adopting the internal regulations of the CNIL;

Pursuant to the decision No. 2013-270 dated 19 September 2013 giving recommendations relative to "digital or electronic safe boxes" intended for individuals;

After having read the report from Mr Jean-François CARREZ, commissioner, and heard the comments of Mr Jean-Alexandre SILVY, government commissioner,

Makes the following comments:

Article 11, 3°, (c) of the Act dated 6 January 1978 amended states that "when requested by professional organisations or institutions of which the members are mainly data controllers, [… the CNIL] delivers a privacy seal to products or procedures intended to protect individuals in respect of processing of personal data, once it has recognised them to be in conformity with the provisions of this [Act dated 6 January 1978 amended].

A request for the creation of a privacy seal relative to digital safe boxes has been made by a professional organisation. The Data Protection Authority considers that this request corresponds to a requirement from stakeholders in this sector.

This requirement by professionals and the CNIL's will to enable the protection of personal data that individuals store in a digital safe box, have led the Data Protection Authority to agree to deliver privacy seals in the matter.

Article 33 of the Data Protection Authority's internal regulations states *"upon proposal from the committee, the Data Protection Authority adopts the standards defining the characteristics that products or procedures must have to allow the delivery of individual certification. These specify the procedures for assessing compliance with the Act and, where applicable, specifics relative to checks following delivery of the privacy seal".*

Consequently, the present decision determines the standard for evaluating digital safe boxes covering the protection of persons with regard to the processing of personal data.

Decides that the standard for evaluating privacy seal requests relative to digital safe boxes is shown in the appendix to the present decision, which is published in the Official Journal of the French Republic.

The Chair

Isabelle FALQUE-PIERROTIN

2.1. Requirements relative to the data processed

APPENDIX

STANDARD FOR CERTIFYING DIGITAL SAFE BOXES

Introduction

The digital safe box, as understood in this standard, covers offers made to individuals concerning services for the dematerialised and secure storage of data, the aim of which is to keep documents on digital media.

Digital safe boxes must ensure the integrity, availability and confidentiality of stored data and implement appropriate security measures.

A digital safe box is distinguished from an ordinary storage space by the fact that the data retained, including stored documents and their meta data, is accessible only to the holder of the safe box and, where applicable, natural persons whom the holder has specifically authorised for this purpose.

The present standard describes the procedures for creation and management, and the content of digital safe boxes. It defines the criteria and the resources allowing the Data Protection Authority to determine whether the digital safe boxes subject to the privacy seal request reach the target objective, namely: the secure retention and protection of personal data contained in a safe box, which will be accessible only to its user and natural persons specifically mandated by the latter.

This standard has been essentially drawn up by the Data Protection Authority based on its recommendations, coherent with the certification processes proposed or being developed by other organisations.

It contains twenty-two requirements, all cumulative, divided into two parts corresponding to two evaluation phases performed by the Data Protection Authority and which cover:

- the applicant's compliance approach, which must, for all processing that it does, ensure the protection of personal data beyond just the service that is the subject of the privacy seal request (two requirements on the approach, noted "ED" in chapter 1);
- the protection of the data in the digital safe box, the subject of the privacy seal request, covering: the data processed, access to the data, retention of data, information to persons, the management of risks and the cryptographic mechanisms (twenty requirements on the service itself, noted "ES" in chapter 2).

Applicants must demonstrate that they satisfy the requirements of the standard by supplying reasoned justification and evidence. These may take the form of an extract

from an internal standard, a description of the functioning of the system or a procedure, or any other document. To be valid, the proposed demonstration must not merely repeat the content of the requirements to indicate that the digital safe box subject to evaluation is compliant with them, but it must establish how the evaluated safe box fulfils them in a specific and detailed manner. Evidence of compliance with requirements ES15, ES17 and ES19 can be given by a description of the algorithms used and the dimensioning chosen, and by appropriate references to appendices B1 and B2 of the general security standard.

The applicant for the privacy seal must be both the technical operator of the service and the supplier of this service to individuals.
We distinguish:

- the manufacturer of the digital safe box product who designs and develops a digital safe box;
- the operator of the digital safe box who implements a digital safe box. To this end, it ensures the operational functioning of the system and related security measures;
- the supplier of the digital safe box who offers this service to users who are natural persons.

Consequently, if the applicant is a legal entity that is both the technical operator of the service and the supplier of the service to individuals, it may request the privacy seal in its name.

On the contrary, when the technical operator supplies the service to an organisation that will play the role of supplier to individuals, it may not be the sole applicant. In this case, the request must be made jointly by both legal entities, the operator and the supplier, to provide all justification and evidence of compliance with the standard necessary to the complete fulfilment of requirements.

Terminology

Digital storage space	Service for storing dematerialised documents.
Digital safe box (synonym of the electronic safe box)	Specific form of digital storage space, in which the availability and integrity of stored dematerialised documents is ensured and only the user (and, where applicable, any natural persons specifically mandated by the user) can

	access the stored documents and their meta data.
Meta data	Data used to describe or manage the stored documents. We distinguish two types of meta data: - meta data created by the user, which is related to a document (such as the name of the document, the format of the document, the document creation date, the document description, the keywords for finding the document); - meta data created by the operator of the digital safe box, which is related to the archiving process (such as the date when the archive was made, the size of the document saved, a hash value of the document saved). In the present document, the term "meta data" covers only meta data created by the user.
Technical operator of the digital safe box	Legal entity which implements a digital safe box. In this respect, it ensures the operational functioning of the system and related security measures.
Supplier of a digital safe box	Legal entity which offers a digital safe box to users.
User of the digital safe box	Natural person who uses a digital safe box.

1. Standard for evaluating the applicant's approach to compliance

ED01. The applicant has set up an approach aiming to ensure compliance with the French data protection act concerning all processing that it performs for all of its activities, including the digital safe box.

ED02. The applicant's processes, including its management of the users of the safe box, have been the subject of appropriate prior formalities with the Data Protection Authority.

2. Standard for evaluating data protection aspects of the digital safe box

2.1. Requirements relative to data processed

ES01. When an account is created, the digital safe box collects relevant and proportionate identification data with regard to the intended purpose. The holder of the safe box may not under any circumstances be identified using the social security number (RNIPP).

ES02. If there is no ministerial approval for hosting health data, the applicant informs the user that it is prohibited to store data related to health. It does not specify the default creation of folders related to health.

ES03. The applicant informs the user that it is prohibited to store illegal content (example: incitement to murder, incitement of racial hatred, child pornography,…).

2.2. Requirements relative to data access

ES04. The digital safe box allows only the consultation of dematerialised documents by the user concerned and, where applicable, any persons specially mandated by the user (such as a notary, to allow rightful claimants to access their data, the spouse when a shared space is created within the digital safe box,…).

2.3. Requirements relative to data retention

ES05. The digital safe box deletes documents that have been definitively deleted by the user, and their meta data, in all places where they are stored:

- without delay for current storage areas and any copies replicated online (mirrored or real-time synchronised);
- within a maximum period of one month for backups (incremental, complete,… performed at a given frequency).

ES06. The applicant ensures the continuity of storage, notably by informing users at least one month before the closure date of the service, to allow them to recover their stored documents.

ES07. The applicant shall make available, without extra charge, a tool allowing users to recover all of the content of their safe box simply, without complex or repetitive actions and in a structured and commonly used electronic format, to facilitate change of suppliers, without collecting any confidential information (such as bank identifiers, passwords for online services, etc.).

2.4. Requirements relative to information on persons

ES08. The applicant first informs the users

- of the identity of the operator of the digital safe box and that of the supplier of the service;
- of the intended purpose(s);
- that there are no addressees of the retained data, including stored documents and their meta data;
- of any envisaged transfer of personal data to a State that is not a member of the European Community, indicating whether this State, based on its own legislation, can make requests to directly access the retained data;
- the rights of persons to access, rectify and object, and the procedures for exercising these rights;
- of the possibility of mandating persons (for example, to allow the user to recover their data in case their key is lost, or their rightful claimants to do so in case of death);
- of the type of space made available to them and its conditions for use;
- of the technical mechanisms used, particularly the encryption mechanisms;
- of the procedures for terminating the service and recovering the stored data;
- in case of a service offer associated with the recovery of documents from third-party services, the consequences of use by the applicant of the identifiers and passwords of users to connect to these services in their name.

2.5. Requirements relative to the management of risks and compliance

ES09. This digital safe box is the subject of an analysis of compliance with the references applicable to the digital safe box, prior to its implementation and then every three years. It includes at least:

- a list of requirements (community, legal, regulatory, sectoral, contractual,…)
- a list of best practices (normative, sectoral standards, internal rules,…) that the applicant undertakes to comply with;
- an explanation of how each applicable reference is complied with, or justification of the fact that it is not.

ES10. The digital safe box is the subject of a study on threats, revised at least every three years. It includes at least:

- all of the threats to which the digital safe box is exposed, namely all of the means which make possible attacks on the availability, integrity and confidentiality of the stored data through the exploitation of IT, physical, human or organisational vulnerabilities, from internal and external sources, whether human or not and whether accidental or deliberate;
- the technical and non-technical measures, put in place or planned, for handling each of these threats by acting before, during or after they occur;
- an estimate of the residual probability of each of these threats.

ES11. The digital safe box includes tools for blocking connections from robots and delaying and/or blocking illegitimate connections made by persons.

ES 12. The digital safe box includes measures aiming to ensure the integrity and availability of data (redundant storage centre, regular backups,…). The applicant makes sure that there are guarantees in terms of compensation for persons in case these measures are ineffective (such as by purchasing insurance with the aim of

covering damage relative to these commitments).

ES 13. The digital safe box includes logging functions enabling users to consult recent activity on their safe boxes (for example by logging and time stamping successful connections and failed connection attempts, the IP address and the protocol used, as well as operations carried out on directories and files, the user who performed an operation, the object on which the operation was carried out and the nature of the operation).

ES14. The digital safe box is subject to independent verification (such as by an external auditor, an internal control service,…) of the effectiveness and efficiency of the measures chosen, at least once every three years, and any corrective measures.

ES15. The applicant shall notify the user in case of any access to their data by a third-party not mandated by the user, even if this data is encrypted.

2.6. Requirements relative to cryptographic mechanisms

ES16. The digital safe box includes a function to encrypt/decrypt the retained data, including the stored documents and their meta data. This function:

- can make the data incomprehensible to third parties not mandated by the user, including to the applicant; to do this, the applicant may, for example, specify and/or supply software to be used on the user's client workstation, specifying the security rules that the user must apply, allowing them to locally encrypt the documents and associated meta data and then send them in encrypted form to the digital safe box, in such a way that the applicant is not technically able to decrypt them;
- allows the user and his/her representatives to decrypt and display the retained data, including stored documents and their meta data;
- is compliant with the rules and recommendations concerning the choice and dimensioning of cryptographic mechanisms in the general security standard from the national information-systems security agency;
- is based on keys controlled by the user and his/her representatives;
- allows evolution of the size of the keys and algorithms used, in order to ensure the long-term confidentiality of the stored data.

ES17. The digital safe box includes a function that facilitates the backup and recovery of encryption/decryption keys to allow the user to continue to access their data if they lose their keys:

- either on the user's premises, in a secured manner;
- or on the premises of a trusted third party, not related to the applicant and chosen by the user; we note that in this case, the trusted third party must ensure the security of the key backups, keep a log of any use of the key backups and inform the user of any use of the key backups.

ES18. The digital safe box includes a function to encrypt all transfers of information to and from the safe box. This function is compliant with the rules and recommendations concerning the choice and dimensioning of cryptographic

mechanisms in the general security standard from the national information-systems security agency.

ES19. The digital safe box implements authentication mechanisms for:

- users;
- natural persons specially mandated by users,
- third parties that users may make use of for importing data from a storage area into the safe box;
- and the IT administrators only for the administration of the safe box.

ES20. The digital safe box only allows authentication using robust authentication mechanisms (single-use passwords, dispatch of codes by SMS,…). It make sure that the user, and the natural persons specially mandated by the user, are authenticated by the server hosting the data. All of these mechanisms are compliant with the rules and recommendations of the general security standard from the National Cybersecurity Agency. If the authentication includes the use of passwords, information about these rules is provided to users (display of the security level of the chosen password, for example) and passwords are also checked (blocking system if insufficient).