Deliberation no. 2017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords

The *Commission Nationale de l'Informatique et des Libertés* (French Data-Protection Authority/CNIL),

Having regard to Council of Europe Convention no. 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to law no. 78-17 of 6 January 1978, as amended, on information technology, files, and freedoms, especially its articles 11, 34, and 35,

Having regard to decree no. 2005-1309 of 20 October 2005, as amended, for implementing law no. 78-17 of 6 January 1978 on information technology, files, and freedoms,

Having regard to deliberation no. 2013-175 of 4 July 2013 on the adoption of the rules of procedure of the CNIL,

After hearing Mr. François Pellegrini, Commissioner, regarding his report, and Ms. Nacima Belkacem, Government Commissioner, on her observations,

Makes the following observations:

Pursuant to article 34 of the law of 6 January 1978, as amended, the data controller is required to take all appropriate precautions, having regard to the data and to the risk presented by the processing, to maintain the security of data and, in particular, to prevent data from being distorted or damaged, as well as to prevent unauthorised third parties from having access to the data.

Similarly, article 35 of the law of 6 January 1978, as amended, specifies that subcontractors and persons acting under the authority of the data controller, or of the subcontractor, must present guarantees that are sufficient to implement security and confidentiality measures referred to in article 34. That does not grant discharge for the data controller from the liability to ensure compliance with those measures.

In that regard, it has emerged from the exchanges that the CNIL has with the data controllers, as part of its consultancy and verification missions, both *a priori* and *a posteriori*, that the means of authentication that is currently the most widespread as part of controlling access to a digital resource is one that links an identifier to a (secret) password.
However, the CNIL has always considered that other means offer greater security, such as two-factor authentication or electronic certificates.

In addition, the increase in IT attacks, which has led to entire databases being compromised, especially those containing passwords associated with the accounts of the persons concerned, has led to an improvement in the attackers' knowledge of passwords.

Finally, the fact that users have the same password for logging in to various online accounts reinforces the obligation that is incumbent upon the data controllers to implement measures that allow the security of personal data.

In that context, and with the aim of creating greater confidence in digital services, it seems necessary for the CNIL to define the technical arrangements of that method of authentication, one that can guarantee a bespoke level of security, and make recommendations concerning the measures to be implemented, as well as the rules to be complied with concerning its use.

To that effect, the CNIL has held talks with its European counterparts as well as with institutions and professionals in charge of information security, in order to build a technical reference framework providing a minimum level of security, one that is consistent with best practice in security matters and that is effectively applicable.

Taking account of those preliminary observations, the CNIL makes the following recommendation, which specifies and applies the provisions of the law of 6 January 1978, as amended, especially articles 34 and 35 thereof.

In order to offer professionals guidelines on managing passwords, the CNIL adopts this recommendation. The latter aims at interpreting the aforesaid legislative provisions, and at informing stakeholders of the implementation of concrete measures to guarantee compliance with those provisions in the state of the art.

I/ Concerning the scope of application of the recommendation

This recommendation concerns all processing of personal data implemented by public or private persons who use authentication by means of a password, except for those for whom specific legislative or regulatory provisions set particular technical requirements.

The recommendation sets minimum technical specifications relating to password-based authentication. In particular, it specifies the arrangements for creating the password, managing the associated account, authentication, retention, changing and renewing the password, and notifying data violations to the person.

The specific risks that processing personal data can bring to bear on the private lives of the persons concerned may require more rigorous measures to preserve data security, such as those concerning the management of IT administrators' passwords or processing sensitive data.

II) Concerning technical arrangements

1) Creating the password and account-blocking

As regards the arrangements for creating a password required for authenticating an account, the CNIL considers that the minimum size and the complexity of that

password must be set by the data controller. In addition, it recommends that the person concerned by the processing must be given prior notification of it by the data controller, as well as of the maximum password size supported by the processing.

There are four possible cases. The first sets strong requirements in terms of password size and complexity. For the subsequent ones, those requirements are less strong, due to the existence of compensating measures aimed at ensuring an equivalent level of security.

In all cases, the CNIL feels that the user should never be given the password in plain text, especially via e-mail.

Case no. 1 – Password alone

If authentication is based only on an identifier and a password, the CNIL considers that:

- the password should have a minimum of 12 characters, and
- the password must include upper-case letters, lower-case letters, numbers, and special characters.

The strength of that authentication is based solely on the intrinsic quality of the user's password. Furthermore, the CNIL feels that the data controller must alert users to that matter, and, to the extent possible, advise them in creating their password.

Case no. 2 – Password and restricting account access

If authentication provides for account-access restriction, the CNIL considers that:

- the password should have at least 8 characters, and
- the password must include at least 3 out of the 4 categories of characters (upper-case letters, lower-case letters, numbers, and special characters), and
- authentication must involve account-access restriction, which must take one or more of the following forms:
    - account-access time-out after several failed attempts, with the length of time-out increasing exponentially over time; the CNIL recommends that the duration should be greater than 1 minute after 5 failed attempts, with a maximum of 25 attempts being allowed every 24 hours; and/or
    - a mechanism that offers protection against automated and intensive authentication attempts (e.g. CAPTCHA), and/or
    - account-blocking after a maximum of 10 consecutive failed authentication attempts.

Case no. 3 – Password and additional information

If authentication includes additional information, the CNIL considers that:

- the password should have a minimum of 5 characters, and
- authentication must involve additional information, which can take one of the following forms:
    - information provided on its own account by the data controller or by the person concerned. The CNIL recommends that the information should contain at least 7 characters, and that it should be known only to the person concerned and to the data controller. If that information is the account identifier, it is recommended that the latter should be specific

to the department (exclusively dedicated), supplied by the data controller, and known only to the person concerned and to the data controller, and/or
    - any technical parameter that is unique to the computer terminal used by the person concerned (IP address, MAC address, user agent, etc.), and for which the person concerned has first established that it is a trusted terminal (e.g. a non-public terminal) that s/he can revoke at any time, and
- account-access restriction must be implemented that can take one or more of the following forms:
    - account-access time-out after several failed attempts, with the length of time-out increasing exponentially over time; the CNIL recommends that the duration should be greater than 1 minute after 5 failed attempts, with a maximum of 25 attempts being allowed every 24 hours, and/or
    - a mechanism that offers protection against automated and intensive authentication attempts (e.g. CAPTCHA). and/or
    - account-blocking after a maximum of 5 consecutive failed authentication attempts.

Case no. 4 – Password and equipment held by the person concerned

If authentication is based on equipment held by the person concerned, the CNIL considers that:

- the password should be at least 4 numbers long, and
- authentication can only involve a hardware device held by the person concerned, i.e. only SIM cards, chip cards, and devices containing an electronic certificate that can be unlocked using a password (token), and
- device-blocking must be implemented after a maximum of 3 consecutive failed authentication attempts.

2) Authentication arrangements

As regards account-authentication arrangements, the CNIL considers that the authentication function must be secure (i.e. that it should use a public algorithm that is known to be strong, and of which the software implementation is free from known vulnerability).

When authentication does not take place locally, the CNIL recommends that a measure to verify the identity of the authentication server should be implemented using a server-authentication certificate. In addition, it is recommended that the communication channel between the authenticated server and the client be encrypted using a secure encryption function (i.e. implementing a public algorithm that is known to be strong, and of which the software implementation is free from known vulnerability). The CNIL also recommends that private keys should be kept secure.

3) Retention arrangements

As regards retention arrangements, the CNIL considers that the password should never be stored in plain text. It recommends that the password for authenticating to a server, and wherever it is technically feasible, be transformed using a secure, non-reversible cryptographic function (i.e. using a public algorithm that is known to be strong, and of which the software implementation is free from known vulnerability), incorporating the use of a salt or a key.

4) Arrangements for renewing the password and notifying the person concerned

The CNIL recommends that the password be systematically renewed if it is compromised.

In all cases, the CNIL feels that the user should never be given the password in plain text, especially by e-mail.

Periodic password renewal

The CNIL recommends that the data controller impose a password-renewal requirement at a relevant and reasonable frequency, which is based in particular on the password complexity required, the data processed, and the risks to which the password is exposed.

It also recommends that the data controller enable the persons concerned to change their passwords themselves. In that case, the rules on password creation shall apply.

Password renewal on request

On request from the person concerned, e.g. in case of a forgotten password, the CNIL recommends that the data controller implement a password-renewal procedure as follows:

- when renewal requires intervention by an administrator, the CNIL feels that the authentication procedure must require the administrator-issued temporary password to be changed on first log-in by the person concerned;
- when renewal is automatic:
  - the CNIL considers that the password should not be transmitted in plain text to the person concerned; it is recommended that the person concerned be redirected to an interface that enables her/him to enter a new password; that interface session should not be valid for more than 24 hours, and it must not enable more than one renewal; or
  - if renewal involves one or more additional items (telephone number, postal address, etc.):
    - the CNIL considers that those items must not be stored in the same storage area as the password-verification item; otherwise, it is recommended that they should be stored in an encrypted form using a public algorithm that is known to be strong, and that the encryption key should be kept secure; and
    - in order to prevent impersonation attempts based on changing those items, the CNIL considers that the person concerned must be immediately informed of their change.

Notification of violation to the person concerned

The CNIL recommends that the data controller notify the person concerned when a violation is detected in relation to the password or renewal-related data (e.g. e-mail address) of the person concerned, within 72 hours of the violation being noted. The CNIL feels that the data controller must require the person concerned to change her/his password at next log-in, and recommends that the person concerned change

her/his password for other departments if s/he has used the same password for the latter.

III) Transitional and final provisions

This deliberation is published in the *Journal Officiel de la République Française* (Official Gazette of the French Republic).

The Chairperson

Isabelle Falque-Pierrotin