Strengthening digital identity solutions with the GDPR

In a context of increasing dematerialisation of administrative procedures and the multiplication of online services, the notion of identity is undergoing profound changes as digital identity emerges, the notion of identity is undergoing profound changes as digital identity emerges. The control of identities by the user and the security of these identities are essential for the protection of personal privacy and the development of trusted digital trusted digital services.

THE INTEREST OF DIGITAL IDENTITY

For the same person, there may be several identities depending on the context (civil status, social and professional life, services online games, etc.) and the level of trust associated with them.

A digital identity can be based on different media: it can be a telephone, a smart card or servers when it is totally dematerialised. when it is completely dematerialised. In many countries, and soon in France, the State provides a national digital identity card which In many countries, and soon in France, the State provides a national digital identity card which makes it possible to extend to the digital world the possibility of proving elements of one's civil status in the physical world.

THE MAIN PRINCIPLES OF THE CNIL REGARDING DIGITAL IDENTITY

The implementation of a digital identity solution necessarily involves the processing of personal data. Therefore, the RGPD is applicable. Given the development of digital identity solutions, here are the main points of vigilance in terms of protection, being reminded that these devices must most often be subject to a data protection impact analysis before their deployment. impact analysis (DIA) before they are deployed, given the stakes for individuals.

The plurality of digital identities

As digital identity is multiple and contextual, it is important to allow individuals to have several digital identities. Thus, an individual should be able to use different digital identities in different contexts (e.g. a so-called "regal" digital identity, which is used to identify a person's identity). identity, linked to civil status and guaranteed by the State, for registering on electoral lists and a digital identity linked to a pseudonym chosen by the individual. a pseudonym chosen by the user for a social network).

The proportionality of the digital identity solution and the importance of pseudonyms

Identification and authentication should be graduated according to the trust needed for each online service. Indeed, it is not It is not necessary to secure all digital identity use cases and it may be simpler for organisations, more user-friendly for users, and more

secure for users.
It may be simpler for organisations, more ergonomic for users and more protective in terms of personal
data processing to adapt the level of security required to the risks associated with the use of digital
identity. risks associated with the use of a digital identity.

In practice, the compulsory use of a strong governmental identity (i.e. the identity guaranteed by
the State at the highest level of insurance) could be limited to of assurance) could be limited to a
small number of cases, while declarative solutions and the use of a pseudonym could be solutions and
the use of a pseudonym could be favoured when there is no particular need for reliability, without
abandoning the imperative of ensuring that the use of all these identities.

Data minimisation

One of the key principles of the RGPD is the principle of data minimisation. It implies ensuring that
only "adequate" data is processed, relevant and limited to what is necessary for the purposes for
which it is processed".

Consequently, when a digital identity is used to access a service, only the information strictly
necessary for the processing envisaged by the service should be provided. service should be
communicated to it. In practice, this means creating or using solutions that give necessary attributes,
for example only a pseudonym or only the first name and year of birth, depending on the nature of the
service used. nature of the service used. New technical solutions that integrate privacy by design not
only provide access to only the necessary attributes, but also allow certain questions to be answered
with only the strictly necessary information (e.g. answering the question "is the person a minor" with
a yes or no rather than sending all the attributes of their civil status).

It is also a question of limiting the information collected by the identity provider. For example, it
is possible to implement decentralised decentralised solutions, which do not allow the identity provider
to know which service a person has connected to.

In addition, it is advisable to favour solutions that integrate privacy protection from the outset and
by default.

Paying attention to the information provided to individuals

Digital identity processing can have a significant impact on the daily life of individuals. In this context,
particular attention should be paid to In this context, particular attention should be paid to informing
data subjects about the processing of their data, whether at the time of enrolment or at the time of
sharing certain identity attributes.

The special case of the use of biometrics

In some cases, biometrics can be used to confirm the link between a civil status

or "regal" identity
and an individual. It can be used at the time of creation of the digital identity, or at the time of
its use. It is also used in some countries to compensate for the lack of properly constituted civil registers.

While the use of biometrics to verify a person's identity or to authenticate him or her to an online service
may seem legitimate, this type of processing is special because it makes it possible to verify a person's
identity or to authenticate him or her to an online service. This type of processing is special because
it involves sensitive data that benefit from a reinforced level of protection. Indeed, the data processed
is consubstantial with the person concerned and cannot be replaced in the event of usurpation or compromise
(an individual can change his password but cannot change his fingerprints). Special attention should therefore
be paid to the conditions of lawfulness of such processing (Art. 9 of the RGPD). In general, storage on
individual media or in a way that allows the individual to control over their data are more protective
for individuals than devices based on a central database of biometric data. biometric data.

REGALIAN DIGITAL IDENTITIES

Regalian digital identities have been subject for several years to the European regulation n¼910/2014 of
23 July 2014, known as eIDAS. This regulation This regulation aims to increase confidence in electronic
transactions and the interoperability of identity systems within the market. To this end, it establishes a
common basis for secure electronic interactions between citizens, businesses and public authorities across
Europe. public authorities across Europe.

In particular, the Regulation sets out requirements for the mutual recognition of electronic means of
identification for exchanges between public sector bodies and users at European level. It defines three
levels of solutions (low, substantial and high) depending on the level of identity verification, thus
allowing for a spectrum ranging from a cursory pre-verification to an in-depth verification and and may
involve various means of authentication (from passwords to smart cards).

A "low" level may be sufficient to register for swimming lessons on the town hall's website, while a high
level may be required for registering the birth of a child. It is good practice to use the lowest level that
guarantees a sufficient level of confidence for a given service.

FranceConnect

Today, eIDAS digital identity solutions are implemented through France Connect, which serves as a bridge
between identity providers (taxes, the Post Office, Ameli, Alicem, etc.) and many e-government services
(town halls, driving licence renewal, etc.) or private services with a regulatory need to verify identity
attributes.

While it should be borne in mind that the inaccessibility of FranceConnect would

have a significant impact
on access to many public services, this architecture has three main advantages:
1 - Identity providers are not aware of the services used by the identity holder.
2 - France Connect can make service providers aware of the importance of identifying the attributes that
are strictly necessary and sufficient for their service, and only transferring them to the service provider,
their service, and transfer only these to them.
3 - France Connect does not require the implementation of a population register dedicated to digital identity
management, even if France Connect performs a verification with the national register of identification of
natural persons.
It should be noted that FranceConnect centralises the technical traces of connection, and that the user can
consult these traces and check whether illegitimate access has taken place.
illegitimate accesses have taken place.

The first high-level identity provider in France: Alicem

Alicem is a mobile application that allows adults with a biometric passport or residence permit to create a
digital identity to access online services such as health insurance, CAF, the "impots.gouv.fr" website, etc.
Initially, the Alicem digital identity can only be used through FranceConnect. This is the first digital identity
solution developed by the State that aims to achieve the high level of security required by the eIDAS regulation.
An experimental phase has been launched in 2019.

In response to a request for an opinion, the CNIL advised the government not to make the use of facial recognition
for enrolment. The CNIL even suggested using alternative solutions to facial recognition to verify the person's identity:
Face-to-face verification of identity: visit to the prefecture, town hall, or a public service that receives the public.
Manual verification of the video and photograph on the document: the video is sent to the ANTS servers and verified by an agent.
Live video call with an ANTS agent.

2021: the year of the digital national identity card?

In application of the European regulation on strengthening the security of EU citizens' identity cards adopted
in June 2019, the government is planning a French digital identity card for 2021.
This card would be both a 'classic' identity card and the medium for a strong digital identity carried by the State.

While technologies have made great strides in recent years, including the development of more protective systems
for personal data, France could be at the forefront of the development of new technologies. France could be at
the forefront of privacy-friendly digital identity by choosing a solution that limits what each entity participating
in its use obtains as personal data to what is strictly necessary. each entity participating in its use
obtains information, whether it be at the creation or use of such an identity.

The CNIL will have to be consulted on the draft texts that will govern the future system. At this stage,
several elements could be taken into account be taken into account:

Certain decentralised architectures make it possible to avoid systematic interaction with the identity provider
when using the service.
As with most uses of identity cards in the physical world, only the service provider and the user are able to
know that the identity is being used at a given time for a given service. In addition, when a higher level of
identification is required, or all uses of the X uses of the identity, a check that the identity has not been
revoked can be implemented.

These solutions could integrate, by design, the use of different identifiers, for example to allow the use of
multiple sectoral identifiers for the public sector. sectoral identifiers for the public sector.
In order to respect the principle of data minimisation, the chosen solution could allow the service provider
to indicate which attributes it needs and ensure that it is able attributes it needs and ensure that only these
are transmitted to it.
The chosen solution could incorporate proof-of-knowledge technologies that allow, for example, to obtain only
proof of majority of the person.