European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 145-152
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 11

*Protection of Personal Data and Digital Identity in relation to the Public Administration: Public Digital Identity System (SpID) in Italy**

Michele Martoni
(Researcher of Legal Informatics – Department of Law – University of Urbino)

ABSTRACT The Italian legislator introduced the Public Digital Identity System (SpID). This tool allows citizens and businesses to dialogue with public administrations. The use of SpID also raises questions about data protection in consideration of the information flows, the subjects involved, and the services provided. This paper outlines the interaction of digital-identities mechanism in the EU context. Finally, it addresses the issue of data protection with a focus on the use of SpID by minors.

1. *From the digital transition to the introduction of the Italian SpID*

Italy has adopted the principle of digital first[1] implemented through the provisions contained in Legislative Decree no. 82 of 2005 (Digital Administration Code or CAD),[2] according to which public administrations must manage administrative procedures using information and communication technologies, must operate through electronic documents and communicate through telematic tools, must accept electronic payments and, moreover, they must guarantee anyone the right to use the services they provide in digital form and in an integrated way, through the telematic tools made available by the public administrations themselves.

The basis of this transition is the National Resident Population Registry (ANPR) governed by Article 62, Legislative Decree n. 82 of 2005, and the related implementing decrees.[3] It is the national database into which the municipal registries will progressively converge.

The ANPR absorbs within itself the National Index of Registries and the Register of Italians Abroad (AIRE). It also contains the computerized national archive of civil-status registers kept by the municipalities, thus creating a single point of reference, a single database, for information relating to personal digital identity.

The Italian legislator, with Decree n. 69 of 2013,[4] amended by Legislative Decree no. 82 of 2005, introduced in our legal system the Public System for the management of Digital Identities (known as SpID).[5] Subsequently, the legislator intervened again, with Decree of 24 October 2014[6] and with Legislative Decrees no. 179 of 2016[7] and no. 217 of 2017[8], to adapt our system to European Regulation no. 910/2014[9] (eIDAS-electronic

* Article submitted to double-blind peer review.

[1] G. Pesce, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, Editoriale Scientifica, 2018.

[2] www.normattiva.it/eli/id/2005/05/16/005G0104/CONSOLIDATED/20220929, last access on 28 September 2022.

[3] For more details see www.anagrafenazionale.interno.it/il-progetto/strumenti-di-lavoro/normativa/, last access on 29 September 2022.

[4] www.normattiva.it/eli/id/2013/06/21/13G00116/CONSOLIDATED/20220929, last access on 20 September 2022.

[5] About SpID, see V. Amenta, A. Lazzaroni and L. Abba, *L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al web*, in *Ciberspazio e diritto*, n. 1, 2015, 11; A. Contaldo, *La disciplina dello SpID (Sistema Pubblico di Identità Digitale) e la definizione giuridica dei gestori*, in *Rivista Amministrativa della Repubblica Italiana*, nn. 9-10, 2016, 541; S. Tura, *Il sistema pubblico di identità digitale*, Bologna, Società Editrice Esculapio, 2017. See also I. Macrì, *L'identità digitale, nuovo documento di riconoscimento*, in *Azienditalia*, n. 3, 2021, 475. See also F. Buccafurri, L. Fotia *et al.*, *Enhancing Public Digital Identity System (SPID) to Prevent Information Leakage*, in A. Kő and E. Francesconi (eds.), *Electronic Government and the Information Systems Perspective*, vol. 9265, Cham, Springer, 2015.

[6] www.gazzettaufficiale.it/eli/id/2014/12/09/14A09376/sg, last access on 10 September 2022.

[7] www.normattiva.it/eli/id/2016/09/13/16G00192/CONSOLIDATED/20220929, last access on 20 September 2022.

[8] www.normattiva.it/eli/id/2018/01/12/18G00003/CONSOLIDATED/20220929, last access on 20 September 2022.

[9] https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32014R0910&from=IT, last access on 20 September 2022. On the eIDAS Regulation, see G. Fi-

IDentification Authentication and Signature), on electronic identification and trust services for electronic transactions in the internal market.

2. *Elements for a better understanding of the SpID*

Italian legislation defines[10] the so-called "SpID digital identity" as "the computer representation of the correspondence between a user and his identification attributes, verified through the set of data collected and recorded in digital form" according to the procedures set out in the implementing decree of Article 64 of Legislative Decree no. 82 of 2005.

To understand the meaning of this definition, it is therefore necessary to refer to the implementing Decree of 24 October 2014, with the *caveat* that the terminology used in Italian law does not correspond to that used in the EU regulation.

In fact, eIDAS Regulation does not use the expression "digital identity", used by the Italian legislator, but the expressions "electronic identification", "person identification data" and "electronic identification means".

Electronic identification means the process of using personal-identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

Personal-identification data means a set of data enabling the identity of a natural or legal person, or of a natural person representing a legal person to be established.

Electronic identification means are a material and/or immaterial units containing personal-identification data, and which are used for authentication for online services.

Lastly, authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.[11]

The first definition that deserves attention is "attributes" (*identifying*, *secondary* and *qualified*), that is an information or qualities of users used to represent their identity, status, legal form, or other peculiar characteristics.[12]

The identification attributes are name, surname, place and date of birth, sex, or company name, registered office, as well as the tax code or VAT number and the details of the identity document used for identification purposes.[13] All this information, moreover, falls into the category of personal data.

The "secondary attributes" are the landline or mobile telephone number, e-mail address, physical and digital address, as well as any other attributes identified by the Agency for Digital Italy (AgID) functional to communications.[14]

Finally, the "qualified attributes" are qualifications, professional ratings and powers of representation and any other type of attributes certified by a qualified authority.[15] This information also falls into the category of personal data.

SpID's actors are the Agency for Digital Italy (AgID), users, identity provider (or IdP), attributes authority, and service provider (or SP).

AgID takes care of the activation of the SpID, carrying out, in particular, the following activities: i) manages the accreditation of the identity and attributes providers, stipulating specific agreements with them; ii) takes care of updating of the SpID register and supervises the work of the subjects participating in the SpID; iii) stipulates specific agreements with those who certify the validity of the identification attributes, that is, the verification of identity documents.

User are those who request the SpID code and who, after obtaining it, intend to access an online service.[16]

SpID identity providers (IdP) are the legal persons accredited to the SpID who, as providers of public services, after identifying the user, assign, make available and manage the attributes used by the same user for the purpose of his/her electronic identification.

The qualified-attributes providers are the subjects accredited by the AgID who have the power to certify the possession and validity of qualified attributes, at the request of service providers.[17]

The service provider (SE) provides

nocchiaro, *Una prima lettura del reg. UE n. 910/2014 (c.d. Eidas): identificazione online, firme elettroniche e servizi fiduciari*, in *Le Nuove Leggi Civili Commentate*, n. 3, 2015, 419.

[10] Translation by the author.

[11] For definitions, see Article 3(1) of eIDAS Regulation.

[12] Cf. Article 1(1)(b) of the Decree of 24 October 2014.

[13] Cf. Article 1(1)(c) of the Decree of 24 October 2014.

[14] Cf. Article 1(1)(d) of the Decree of 24 October 2014.

[15] Cf. Article 1(1)(e) of the Decree of 24 October 2014.

[16] Cf. Article 1(1)(v) of the Decree of 24 October 2014.

[17] Cf. Article 1(1)(m) of the Decree of 24 October 2014.

Information Society services[18] or services that administrations and public bodies provide users through online information systems. The SE forwards users' electronic identification requests to the IdP.[19]

I note that the IdP is qualified as a "public service provider" and that it is expressly assigned the task of carrying out users' identification.

This task is reiterated in Article 7 of Decree of 24 October 2014, which states that digital identities are issued, at the request of the interested party, by the identity provider, after verification of the identity of the applicant.

The provision then specifies the methods for verifying the identity of the applicant.

The Decree of 24 October 2014 then regulates (i) the identification code, (ii) the access credential and (iii) computer authentication, linking them to the computer (or electronic) identification procedure.

The identification code is a particular attribute assigned by the IdP which allows to uniquely identify a digital identity in the context of the SpID. This is a unique code, which is assigned by the provider of the SpID code, and which can take, for example, a format like "INFC0000052141".

The access credential is a particular attribute used by the user, together with the identification code, to securely access, through electronic authentication, the qualified services provided by suppliers of services that adhere to the SpID.[20] Article 1(1)(r), of the Decree of 24 October 2014, specifies (incidentally) that the credentials are "chosen".

Electronic authentication is the verification carried out by the IdP, at the request of the SE, of the validity of the access credentials presented by the users to the same provider, to validate their electronic identification.[21]

Article 6 of the Decree of 24 October 2014 provides that the SpID is based on three levels of authentication security:

a) at the first level, corresponding to the Level of Assurance LoA2 of the ISO/IEC DIS 29115 standards, the digital identity provider makes available one-factor computer authentication systems, such as passwords;

b) at the second level, corresponding to the Level of Assurance LoA3 of the ISO/IEC DIS 29115 standards, the digital identity provider makes two-factor authentication systems available, not necessarily based on electronic certificates, whose private keys are kept on devices that meet the requirements of Annex 3 of Directive 1999/93/EC of the European Parliament;

c) at the third level, corresponding to the Level of Assurance LoA4 of the ISO/IEC DIS 29115 standards, the digital-identity provider makes available two-factor authentication systems based on electronic certificates, whose private keys are kept on devices that meet the requirements of Annex 3 of Directive 1999/93/EC of the European Parliament.

The SpID code has its own life cycle that needs to be managed and monitored.

In particular, users must keep their attributes valid and updated.

The code may be subject to suspension and revocation, for example in the event of the user's death, termination of the legal entity, non-use for more than twenty four months, illegal use of the SpID code, contractual expiry or request of the user.

Below are two figures illustrating, respectively, the SPID application procedure and the procedure for requesting access to a service issued by a service provider.

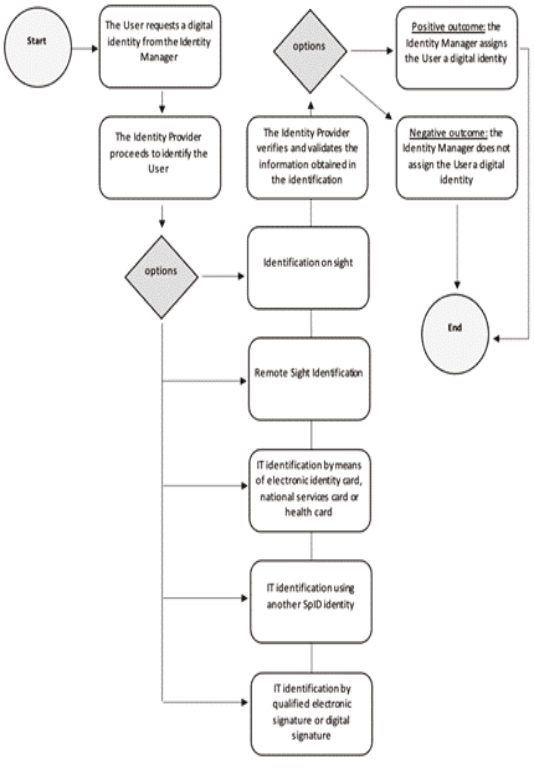

Figure 1. Application procedure

[18] Cf. Article 2(1)(a) of Legislative Decree no. 70 of 2003.
[19] Cf. Article 1(1)(i) of the Decree of 24 October 2014.
[20] Cf. Article 1(1)(h) of the Decree of 24 October 2014.
[21] Cf. Article 1(1)(f) of the Decree of 24 October 2014.

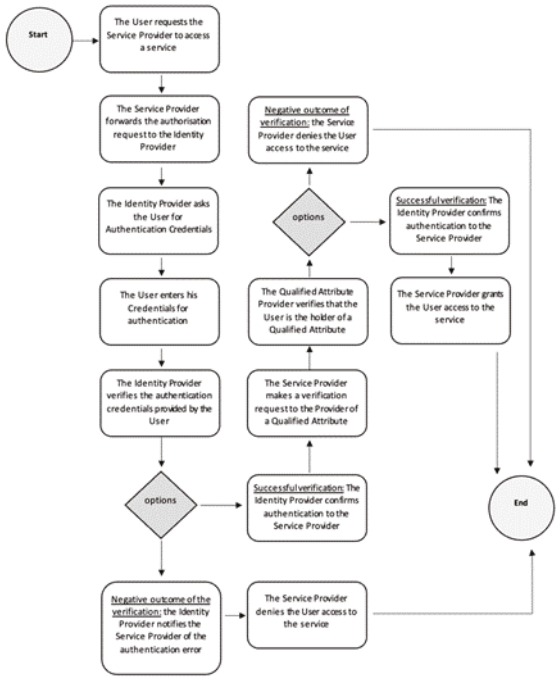

Figure 2. Procedure for service access

3. *The Italian eIDAS node (FICEP)*

The FICEP project (First Italian Cross-border eIDAS Proxy) has been financed by the European Commission under the CEF-Telecom eID 2014[22] call for proposals and is aimed at implementation of the Italian eIDAS node.

On 12 May 2017, the Directorate General for Informatics (DIGIT) of the European Commission notified AgID of the successful completion of validation tests on the correct implementation and interoperability of the national node, the implementation of which will enable the circulation of Italian digital identities (SpID) among the Member States of the European Union and *vice versa*.

Thanks to the FICEP project, with the implementation of a national eIDAS node, it will therefore be possible for Italian citizens to access the online services of other EU countries and, at the same time, for European citizens in possession of national electronic identification tools recognised under eIDAS to access the services of Italian public administrations.

The cross-border electronic identification process can be schematized as follows:

(1) the Italian user requests access to the service of an EU Member State;

(2) the service provider of the Member State sends a request to its own eIDAS node;

(3) the eIDAS node of the Member State asks the Italian user his/her country of origin;

(4) when the user selects his/her country of origin, the Member State's eIDAS node sends a request to the Italian eIDAS node; (5) the Italian eIDAS node responds to the Member State's eIDAS node's request by querying the provider of the applicant's SpID digital identity, for electronic authentication;

(6) once the electronic authentication is successful, the Italian eIDAS node sends a confirmation to the Member State's eIDAS node, which in turn forwards the confirmation to the Member State's service provider;

(7) the Member State's service provider allows the Italian user access to the requested service.[23]

4. *Instances and declarations submitted to the Public Administration by telematic means*

The Digital Administration Code provides a broad definition of services that can be delivered online, which are qualified as any service of a public administration that can be used at a distance by electronic means.[24] What these services are is not, however, indicated with a precise listing.[25]

Article 65 of the Italian Digital Administration Code (CAD) regulates the validity of instances and declarations submitted electronically to public administrations and public-service providers in general.

The Italian legislator has regulated how the telematic application must be formulated to be valid.

The first case considered by the Italian legislator requires the instance or declaration to be signed by one of the methods set out in Article 20 (CAD), which regulates the different types of electronic signatures.

Instances and declarations submitted

[22] See *www.agid.gov.it/it/piattaforme/eidas/progetto-ficep*, last access on 10 September 2022.

[23] See http://www.agid.gov.it/it/piattaforme/eidas/progetto-ficep, last access on 20 September 2022.

[24] See Article 1(1)(n-*quater*) of Legislative Decree no. 82 of 7 March 2005.

[25] On the use of information technology in the provision of public services, see A.G. Orofino and F. Cimbali, *L'uso delle tecniche informatiche nella prestazione di servizi pubblici*, in *Giurisprudenza Italiana*, n. 6, 2022, 1507; M. Martoni, *Servizi online della pubblica amministrazione: l'informatizzazione della dichiarazione di inizio attività in materia edilizia*, in *Ciberspazio e Diritto*, n. 11, 2010, 5.

electronically to the public administration are also valid when the applicant or declarant has been identified through the Public Digital Identity System (SpID), or through the Electronic Identity Card (CIE) or the National Services Card (CNS).[26]

Article 65 (CAD) provides that instances and declarations are valid even if: formed through the telematic access point for mobile devices referred to in Article 64-bis of the CAD; or signed and submitted together with a copy of the identity document; or if transmitted by the instant or declarant from his/her digital domicile registered in one of the lists referred to in Article 6-bis, 6-ter or 6-quarter (CAD) or, in the absence of a registered digital domicile, from an electronic address elected as a certified electronic mail service or a qualified certified electronic delivery service, as defined by the eIDAS Regulation.

5. *The Italian Data Protection Supervisory Authority about SpID*

The Italian Data Protection Supervisory Authority has intervened on several occasions on the SpID regulation.[27] Eight opinions have been issued since 2014. Among others, I would point out, in particular: the opinion on a model convention scheme for private service providers (29 September 2016); the opinion on a model convention scheme relating to the adherence to SpID by public administrations, in their capacity as service providers (18 February 2016) and the opinion on a draft regulation on the implementing modalities for the implementation of SpID and a draft convention relating to providers (17 December 2015); the opinion on two draft regulations containing, respectively, the implementing modalities for the implementation of SpID and the related technical rules (4 June 2015); the opinion on an outline of regulations setting out the procedures necessary to enable digital-identity providers, through the use of other IT identification systems that comply with SpID requirements, to issue digital identities (23 April 2015); the opinion on an outline of regulations setting out the procedures for the accreditation and supervision of digital-identity providers (23 April 2015); and, finally, the initial opinion on the outline of the decree of the President of the Council of Ministers on the public system for managing the digital identity of citizens and businesses (19 June 2014).

On 17 September 2020, the Italian Supervisory Data Protection Authority issued a further opinion on the new methods for issuing digital identities through remote recognition, which no longer require the simultaneous presence of the SpID operator and the applicant.

As I have already illustrated, the use of SpID implies the processing of personal data both at the time of registration and at the time of access to services.

I have also tried to graphically represent how SpID implements a flow of information – including personal data– involving various public and private entities.

This implies the need for a deep analysis during implementation for the correct allocation of roles (for example data controller and data processor) with respect to the figures envisaged by the GDPR, both regarding the identity provider and the service provider or attribute provider. This allocation of roles will have to find its own regulation in legal acts between the parties involved, and an adequate level of information and transparency with respect to the data subject will also have to be guaranteed.

It will also be necessary to ensure compliance with the fundamental principles[28] of data processing at every stage of the process.

One issue that emerges is the quantity and quality of data shared between identity providers and service providers. The proper implementation of the principles of necessity and data minimisation requires, in fact, that only data that are strictly indispensable with respect to the purpose of the processing set by the data controller should be exchanged between the two parties.

Providers must also guarantee, among other things, the principle of confidentiality and the

[26] See M. Martoni, *Identità personale anagrafica (autorizzata) vs identità personale autorappresentativa (manifestata)*, in *Rivista Trimestrale di Diritto e Procedura Civile*, n. 1, 2020, 179; M. Nastri, *Identità personale, identità digitale e identificazione elettronica alla luce del decreto semplificazioni*, in *Notariato*, 6, 2020, 608; F. Arcieri, M. Ciclosi, A. Dimitri, *et al.*, *The Italian Electronic Identity Card: overall Architecture and IT Infrastructure*, in F. Nardelli and M. Talamo (eds.), *Certification and Security in Inter-Organizational E-Service*; in *IFIP On-Line Library in Computer Science*, vol. 177, 2005.

[27] https://www.garanteprivacy.it/temi/pubblicaamministrazione-e-trasparenza/spid, last access on 28 September 2022.

[28] See Article 5, GDPR.

principle of data integrity by adopting appropriate and adequate security measures in this respect.

I will not dwell further on these general profiles. Rather, I would like to direct my attention to a particular implementation of the SpID that raises issues regarding the processing of personal data. I intend to refer to the possibility of assigning the SpID digital-identity to minors.

5.1. *SpID and protection of Children's Personal Data*

With Determination no. 353 of 3 May 2021, AgID issued the operational guidelines for the use of SpID services by children concerning the issuance of digital identities and related methods of use for accessing online services. At the same time, AgID also launched a public consultation on the text of the guidelines, which ended on 14 June 2021.[29]

On 2 February 2022, the Italian Data Protection Supervisory Authority delivered to AgID its opinion on the draft guidelines[30] with the aim of outlining guarantees for the use of SpID by children.[31]

On 3 March 2022, AgID adopted Determination no. 51, which ultimately adopted the operational guidelines for the use of SpID services by children.[32] Subsequently, with Determination no. 133 of 11 May 2022, AgID issued some changes by publishing a second version of the guidelines.[33]

More specifically, the guidelines define: (i) how to issue a digital identity to the child; and (ii) how to use online services through this identity.

About (i) I describe below the procedure for issuing SpID in favour of a child:

(1) The IdP (Identity Provider) offers its users a service dedicated to the request for the issue of SpID in favour of children and provides specific information on the processing of the minor's personal data for the purpose of issuing and managing the digital identity, pursuant to Articles 12 *et seq.* of the GDPR;

(2) The parent, among other things, accesses, with level 2 credentials, the service made available by the IdP; enters the data relating to the minor for whom SpID is being requested (name, surname, tax code, date of birth) and declares that he/she exercises parental responsibility over the child;

(3) the IdP generates the "parent code" and then the "verification code" assigned to the child, then communicates it to the parent;

(4) the parent communicates the verification code to the child outside the IdP channels. The child communicates the verification code to the IdP;

(5) the IdP verifies the parent's authorisation to issue the SpID and, if positive, identifies the minor, verifying the correspondence of his/her identity with the data previously provided by the parent. The IdP then issues the digital identity to the minor and sends a notification to the parent, indicating the name of the minor for whom the SpID has been issued.

Let me now turn to point (ii). In this regard, AgID emphasises that service providers – before providing a service to children through SpID– must make an independent, reasoned, and demonstrable assessment of the need to:

[29] For more on the public consultation see https://docs.italia.it/AgID/documenti-in-consultazione/lg-spid-minori-docs/it/bozza/index.html, last access on 29 September 2022.

[30] For the Opinion of the Italian Data Protection Supervisory Authority www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9744322, last access on 29 giugno 2022.

[31] In his opinion, the Supervisory Authority for the Protection of Personal Data requested AgID to amend the scheme by introducing additional guarantees, particularly regarding the procedure for issuing SpID identities by Identity Providers. The Authority requires an accurate verification of the identity of the parent and the child and the identification of the information to be collected and stored, in compliance with the principle of minimisation. Service Providers will also have to undertake to assess which services to offer directly to minors and the guarantees to be ensured in view of their characteristics. The use of SpID for children under the age of 14 (and from the age of five), is only admissible for online services offered by schools (such as, for example, the electronic register) and will have to take place for an experimental period, until 30 June 2023, while still guaranteeing access to these services without SpID with the methods that may already be in use. At the end of the trial, which will also involve the Ministry of Education, the adequacy of the measures adopted will have to be assessed. Moreover, the information addressed to minors, in accordance with what is already provided for in Article 12 of the GDPR, will have to have simple and clear language. AgID will also have to send a report to the Supervisory Authority on the use of SpID by minors, indicating the services offered, the number of identities issued, any critical issues detected, and the measures identified to remedy them. For further details, see the text of the opinion already mentioned and referred to in the previous footnote.

[32] For Determination no. 51 of 3 March 2022, see https://trasparenza.agid.gov.it/index.php?id_oggetto=28&id_doc=123125, last access on 29 august 2022.

[33] For Determination no. 133 of 11 May 2022, see https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_123194_725_1.html, last access on 29 august 2022.

(a) know the minor's age; (b) obtain certainty of the user's identity for the purposes of the service.

Chapter nine of the guidelines dedicated to the protection of personal data, specifies that AgID's indications are explicitly oriented towards the concrete application of the principles underlying the protection of personal data under Article 5 of the GDPR, the procedures identified for the issue and management of the child's digital identity and for the use of the services.

With a view to maximum protection of the child's personal data, SpID allows service providers –when they deem it appropriate based on their own evaluations, in compliance with the principle of accountability– to obtain certainty as to the age of the child even in the absence of any other data that could further identify him/her. The SE could, for example, request only the attribute attesting to the minor's date of birth without any other identifying information.

This would make it possible, on the one hand, to verify that a child is not accessing inappropriate content but, at the same time, it would make it possible not to expose him or her to data processing resulting from the use of the service for which he or she would essentially be anonymous. This modality is in the groove already traced by the CNIL[34] and the ICO.[35]

6. *An evolving scenario*

The European Commission presented on 3 June 2021 a proposal to amend the eIDAS Regulation with which it aims to introduce the so-called *European Digital Identity Wallet.*[36]

The European Digital Identity Wallet would combine, in a mobile environment, the national electronic identification solutions – introduced so far by the Member States in implementation of the eIDAS Regulation– with the digital attestation of personal attributes (e.g., possession of a driving licence, educational qualifications, medical prescriptions).

The proposed regulation will therefore impose an obligation on Member States to develop their own solution based on common technical interoperability and security standards that the Commission will publish within six months of the entry into force of the amendment to the Regulation.

The existing legal framework for digital identities, i.e., the current version of the eIDAS Regulation, provides the basis for cross-border electronic identification, authentication, and certification of websites within the Union.

However, there is no obligation for Member States to develop a national digital ID and make it interoperable with those of other Member States, which leads to large discrepancies between countries.

Hence the sense of the current Commission proposal that attempts to address these shortcomings by improving the effectiveness of the framework and extending its benefits to the private sector and mobile use.

The use of the European Digital Identity Wallet –according to the intentions of the Commission proposal– is to be used with respect to (i) the public administrations of the Member States, even if the European Digital Identity Wallet is issued by another Member State, (ii) private service providers using strong authentication systems by virtue of legal or contractual obligations, and, finally, (iii) large digital platforms (as they will be better defined in the Digital Service Act[37]).

The new Wallets will therefore allow all Europeans to access online services without having to use private electronic identification

[34] See www.cnil.fr/en/home, last access on 29 September 2022.

[35] See https://ico.org.uk, last access on 29 September 2022.

[36] For the proposed amendment, see https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52021PC0281, last access on 11 September 2022. For further study see also https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en, last access 11 September 2022. In this context, it is worth mentioning the Commission's strategy called *Digital Compass 2030* (see https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en, last access on 29 September 2022. See also https://futurium.ec.europa.eu/en/digital-compass, last access on 25 September 2022. Among the targets of the strategy, 80 per cent of citizens should use an eID solution in 2030.

[37] On 24 March 2022, a provisional political agreement was reached between the Council and the Parliament on the regulation of digital markets. Approval by Coreper followed on 15 June 2022. The current text is available at: https://data.consilium.europa.eu/doc/document/ST-9342-2022-INIT/x/pdf, last access on 29 September 2022. It will apply to all online intermediaries providing services in the EU. As the obligations introduced are proportionate to the nature of the services concerned and adapted to the number of users, very large online platforms and online search engines will be subject to stricter requirements.

methods or share (where not necessary) personal data.
On the other hand, if on the one hand the use of the European Digital Identity Wallet will minimise the need to communicate users' personal data to digital service providers, on the other hand the creation of a single system containing not only the digital identities of European citizens and residents within the European Union, but also other personal data (including special categories of personal data) and documents, will pose the need to ensure a very high level of security to avert the risks of access and misuse of information and identity theft.
It is interesting to mention the European project Electronic Identification and Trust Services for Children in Europe (euCONSENT).[38]
It was financed in the Programme Pilot Project and Preparatory Actions (PPPA-2020), dedicated to the implementation of child rights and protection mechanisms in the online domain based on the GDPR and other relevant EU legislation.
The objective of the project is to establish an interoperable technical infrastructure dedicated to the implementation of child-protection and parental-consent mechanisms based on EU legislation.
The technical measures will be based on the use of electronic identification means (in particular, electronic identification schemes notified by the Member States under the eIDAS regulation).
To do this, the euCONSENT project aims to carry out a large-scale mapping of existing age verification and parental consent collection methods in the context of online child protection.
Mapping should allow the identification of good practices, including those that ensure compliance with the current regulatory framework.
Subsequently, based on a mapping evaluation, the project will focus on designing, implementing, and testing an interoperable infrastructure for online child protection, including age verification and collection of parental consent of users of video-sharing platforms or other similar online services, using different approaches.

[38] For further details on the project euCONSENT, see https://euconsent.eu, last access on 20 September 2022.