POSEIDON

Protection and control of Secured Information by means of a
privacy enhanced Dashboard

GRANT AGREEMENT NUMBER: 786713
H2020-DS-2016-2017/ DS-08-2017

Deliverable

D8.2 – Report on privacy and associated legal EU framework

List of Acronyms
AB Advisory Board
CA Consortium Agreement
EB Executive Board
EC European Commission
GA General Assembly OR Grant Agreement
PC Project Coordinator
TL Technical Leader
WP Work Package
WPL Work Package Leader

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786713.

Report on privacy and associated legal EU framework

Project Title:	**POSEIDON**

Deliverable Number:	D8.2
Grant Agreement number:	786713
Funding Scheme:	HORIZON 2020
Project co-ordinator name:	Francesco Paolo Schiavo – MEF (Italian Ministry of Economy and Finance)
Title of Deliverable:	Report on privacy and associated legal EU framework
WP contributing to the Deliverable:	WP8 Ethical Monitoring
Deliverable type	R - Report
Dissemination level	PU - Public
Partner(s)/Author(s):	Dario Reccia, Giovanni Maria Riccio, Adriana Peduto, Maria Pia Verzillo – E-LEX

History:			
Ver.	Comments	Date	Author
0.1	First draft	18/09/2018	E-LEX
0.2	Draft internally reviewed	12/10/2018	E-LEX
0.3	Version ready for internal peer review	17/10/2018	E-LEX

Project funded by the European Commission Horizon 2020 -
The EU Framework Programme for Research and Innovation.

The POSEIDON Consortium consists of:

Table 1 - Consortium Partners

Logo	Name	Country
	MEF – Ministero dell'Economia e delle Finanze	Italy
	ACN - Accenture S.p.A.	Italy
	PNO – PNO Innovation	Belgium
	E-LEX – e-Lex Studio Legale	Italy
	TECN – Fundacion Tecnalia Research & Innovation	Spain
	SAN – Ayuntamiento de Santander	Spain
	SOFT - Softeam	France
	UC – Universidade de Coimbra	Portugal
	BRZ - Bundesrechenzentrum GmbH	Austria
	JIBE – SMARTFEEDZ B.V.	Holland

TABLE OF CONTENTS

1 Summary

PoseID-on aim is to develop and deliver an innovative intrinsically scalable platform, namely the ***Privacy Enhancing Dashboard for personal data protection***, as an integrated, collaborative, trustable and innovation-focused ecosystem platform, through which governments openly collaborate with citizens, companies, other government organizations for the sake of service delivery, in compliance with guaranteeing, at the same time, subjects fundamental rights.

The PoSeID-on Privacy Enhancing Dashboard is thus an integrated and comprehensive IT solution, ensuring the following:

- **Empowering data subjects** in having a concise, transparent, intelligible and easy access, as well as tracking, control and management of their Personally Identifiable Information (PII) processed by public and private organizations, acting as data controllers and/or data providers. They will be able to make conscious decisions about who can process their own data, by enabling, restricting or revoking permissions in accordance to the data minimization principle, as well as to be alerted in case of privacy exposure.
- **Supporting public and private organizations** to guarantee fundamental rights of data subjects and to properly **respond to the new EU regulations** by also gaining substantial advantages for their own activities, enforcing their traditional procedures.

Therefore, the PoSeID-on Privacy Enhancing Dashboard is aimed to safeguard the rights of data subjects (i.e. all those natural persons that represent the primary target of the EU Regulation on Data Protection - GDPR), as well as support organizations in data management and processing while providing electronic services and ensuring GDPR compliance. Access to the Dashboard is ensured through the use of the electronic IDentification (eID) accounts. The platform is thus open to Digital Identities and Access Management managed according to eIDAS Regulation (electronic IDentification, Authentication and trust Services, the EU regulation on electronic identification and trust services for electronic transactions in the internal market).
In this context, the current deliverable aims in **section 2** to describe the current EU legal framework relevant for the PoSeID-on platform on privacy and data protection. The current EU data protection legal framework for privacy and data protection is composed mainly of two legal instruments: the GDPR on May 25, 2018, which sets conditions for the processing of personal data; and the ePrivacy Directive 58/2002 (hereinafter "ePrivacy Directive"), which provides specific rules for the electronic communications sector. Notably, in cases of conflict with the GDPR, the rules of the Regulation would prevail.

Finally, **section 3** illustrates the European legal framework with reference to the digital entity, showing current practices in the project pilots member states (Italy, France, Spain and Austria).

2 General introduction to the EU legal context on privacy and data protection

2.1 The privacy concept before the General Data Protection Regulation

The European General Data Protection Regulation (hereafter: GDPR or just Regulation) sets a new standard for data collection, storage and usage among all companies that process the personal data of subjects who are in the European Union (hereafter: EU). It changes how companies handle privacy, and enforce people's rights to access and control their own data.

The right to privacy firstly arose as a right to be let alone1, thus the right to exclude others from subject's personal sphere. For a long time privacy was consider as a way to avoid the interference of public agencies in private life.

Specifically, inside the European Union, the concept of privacy made its first appearance in 1950 with the EU Convention on Human Rights. It stated on its Article 8 that everyone has the right to respect for his private and family life, home and correspondence. In addition, also limited public agencies interference in private life and established some cases in which the action of a public authority would be acceptable.

This concept of privacy, however, changed over the years.

Considering the technological changes and in the presence of digital revolution, the right to privacy started to be seen more as a right to control personal information. In fact, in 1980, The Organization for Economic Co-operation and Development (hereafter: OECD) issued guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These non-binding principles had a dual aim of setting minimum standards of privacy and data protection, and of eliminating restrictions on transborder data flows. For the first time, personal data was defined as "any information relating to an identified or identifiable individual".

The guidelines were endorsed by both EU and US and were the basis of many national laws regarding data privacy, even if at the time privacy regulation and the levels of data protection varied greatly amongst different countries.

In 1981, the Council of Europe presented the Convention 108, which consisted in the only international treaty – at the time - with legally binding character that dealt specifically with data protection.

Even so, it was only in 1995 that the European Commission approved a directive, called the Data Protection Directive (hereafter: DPD, Directive 95/46/EC or just Directive) to regulate the processing - including the collection, use, storage, disclosure and destruction - of personal data. Personal data definition given by the DPD was the same definition used for the OECD guidelines and applied to all personal data collected for or about EU citizens.

[1] In 1890, when two lawyers, Samuel D. Warren and Louis Brandeis, published in the Harvard Law Review an article called "The Right to Privacy". The phrase "right to be let alone" since then became the definition of privacy.

The Directive intended to guarantee the fundamental right to privacy by introducing minimum standards for the use of personal data. It sought to harmonize European member states data protection laws, providing a regulatory framework that secured free movement of personal data, setting a baseline of security around personal information whenever it is stored, transmitted or processed. It was implemented by all the EU member states, plus Norway and Liechtenstein and it came into force in October 1998.

It is important to highlight that Directives are not an instrument with binding legal force itself. It only sets aims, objectives or results to be achieved by each European member state. That is the reason why, even though its implementation, data protection laws would still vary among the European countries.

According to the Directive, processing data is defined as "any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". Moreover, every subject handling data should always respect the following principles:

a) Fair and legal process – personal data must be processed fairly and lawfully.

b) Purpose-limited – personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".

c) Relevant – personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."

d) Accurate – personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard for the purposes for which they were collected or for which they are further processed, are erased or rectified."

e) Time-limited – personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which are further processed".

Furthermore, the Directive also granted data subjects the right to access (understood as the right to obtain information regarding whether their personal data is being processed, the content and the source of any personal data undergoing processing and the purpose of any processing) and to correct, erase or block the transfer of inaccurate or incomplete data. Finally, has also determined the creation of a national supervisory authority in each member state.

For almost 20 years, the DPD remained as a reference of good practice on data protection, having a positive impact in structuring and organising the debate surrounding the subject. The Directive had an important role not only inside the EU, but it was also internationally respected and often held up as a standard for good data protection practices even in contexts where it was not directly applied.

However, a review of rules was definitely needed: in the past two decades, internet and technology suffered big advances and deeply transformed the way we interact with each other. Thus, the aim of the GDPR is to enable people inside the EU to have a better control over their personal data and to guarantee the protection of their data as a fundamental right.

2.2 The General Data Protection Regulation

The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, hereinafter: GDPR) has been issued on 27th April 2016 and is in force in all EU members from 25th May 2018.

The text is composed by 99 articles plus 173 recitals. It is a complex text which aims, on one side, at updating the European legislation on data protection with a legislative act which is more adequate to the modified technological and sociological scenario and, on the other hand, to adopt a text which will be enforceable, without differences, in all the member States. In fact, being the GDPR a regulation, it does not require an implementation by the member States into their national legal framework.

The GDPR has, among its purposes, that of *"ensuring a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data in the Union".* This purpose of harmonisation has not been achieved by the previous EU directives and notably by the Directive 46/97/EC, although it is regarded as a central issue by the same European Institutions. The option of adopting a Regulation instead of a Directive aims at ensuring a common framework, limiting the regulatory interventions by member States and national data protection authorities.

However, a limited State legislative power still remain, as some sectors do not fall into the scope of the GDPR, such as: freedom of expression and research; labor law; access to official documents.

The GDPR has followed a complex path before its formal and final approval. It has been proposed on January 2012, then on March 2014 the European Parliament has issued and amended version, as well the Council of Europe, on June 2015.

The approach of the GDPR, if compared with the previous legislative acts of the European institutions, contains a significant innovation, as it combines the strictly regulatory aspects with organizational and technological aspects.

2.2.1 Personal data and personally identifiable data

GDPR defines (article 4, par. 1) the personal data as *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or will more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Article 4 of the GDPR includes definitions of specific personal data, which are mostly related to sensitive and peculiar aspect of the personality of physical subjects, and notably:

- genetic data: *personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of*

that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question [article 4, n. (13)];

- biometric data: *personal data resulting from specific technical processing relating to the physical, physio- logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data* [article 4, n. (14)];
- data concerning health: *personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status* [article 4, n. (15)].

Furthermore, processing of personal data being able to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are, in general, prohibited and may be processed exclusively in some specific cases. These categories of personal data are subject to additional protections, as they are considered as the hardcore of the protection that must be ensured to citizens by privacy regulations.

The general principle is that personal data can be processed if the data subject has provided his consent to the processing of his or her personal data for one or more specific purposes. However, the GDPR lists several cases in which personal data may be processed based on other circumstances and prerequisites, such as where processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

Anonymous information are not covered by the EU Regulation. Whereas n. 26 states that "*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes*".

The GDPR makes a distinction between the anonymization and the pseudoanonymization. The latter refers to reversible de-identification of personal data, for example in cases where it is possible to re-identify hashed identifiers.

Furthermore, according to Whereas n. 26 of the GDPR, "*The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural*

person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".

It is a crucial point for the use of big data as personal data, once anonymized (or pseudo-anonymized), may be freely processed, without any prior authorization by the data subject.

The GDPR, even if not defining the anonymized data, includes a definition of pseudononimization which means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

2.2.2 Data roles

The GDPR provides the definition of data subject, data controller, data processor, third party and recipient.

Within the data protection regulation, the data subject is a living individual and a natural person to whom personal data are referred.

The data controller (or simply the "controller") is the subject (natural person or legal entity), public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In other words, the data controller is the one who is directly responsible for the processing, for its purposes, for the security measures, and so on.

The data controller may appoint some of the processing tasks to another subject, qualified by the GDPR as "data processor" (or simply "processor"), who processes personal data on behalf of the controller. The processor may be an internal subject belonging to the entity which acts as controller or an external subject (e.g. the company who is in charge for security measures; suppliers of external services, etc.).

Personal data may be disclosed to other subjects. In this case their role, in the context of GDPR, is defined as recipient, i.e. a "*natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not*".

Finally, the third party is defined by the GDPR as "*a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data*".

Moreover, recipient means *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing".*

2.2.3 Material and Territorial Scope

The GDPR has improved the material and territorial scope of the Directive 95/46/EC. In particular, the GDPR is applicable to natural persons, but not to anonymized data, i.e. the data which do not allow to identify a data subject.

As for the territorial scope, it covers the cases where the controller is established within the EU territory, but also the case in which the controller is established outside the EU territory if it offers goods or services to data subjects in the Union or just monitors their behaviour as it takes place within the Union. In other words, the GDPR is applicable also to companies (such as many new economy companies) even if they are not based in Europe, once they provide services or goods to European citizens.

In any case, the GDPR does not define the criteria and the processes to anonymize personal data. These techniques are listed in the Opinion no. 05/2014 of 10 April 2014 of the Working Group Article 29 and include, for instance:

- *Randomization with added statistical noise*: Spatial and temporal. It changes the authenticity of personal data by decreasing spatial accuracy by associating the covered area, which ranges from several hundred square meters to a few square miles. Over time, authenticity is diminished from the moment of detection to its time bands.
- *Generalization*: The only attributable data associated to the person is the nationality of origin and the region, province or county (if of large dimension) of statistical residence. This attribute does not allow the identification of any person within the region or country of origin. Even this measure is compliant with the indications of the abovementioned Opinion no. 05/2014.
- *K-anonymity*: it comes out from the choice of generalization and in the most urgent case it corresponds to the number of the universe of reference. Example: if the attendance of people from Milan in Florence is on average of 1,000 per day, the only thing known is that they belong to the 4 million people statistically resident in Rome or Madrid.
- *L-Diversity*: In cases where analysis for any reason should be lower than the threshold of 10 units, these analysis are aggregated to other classes (for example, all nationalities with less than 10 units are aggregated as foreigners). If this is not possible (e.g. in destination origins) analysis are targeted as "data not available".
- *Differential Privacy*: The used models also allow permutation/translation of behavior within the area/period of interest without modifying the results. This applies to average attendance (1 person-hour = 2 people-half-hour = 6 people-10minutes) and to movements / co-visits (100 movements A> B every Monday of the month = 400 movements on Monday and none in the other Mondays).

2.2.4 Principles of data processing

The processing of personal data must comply with the some specific principles. In particular, personal data must be:

- *processed lawfully, fairly and in a transparent manner*
- *collected for specified, explicit and legitimate purposes*
- *limited to what is necessary*
- *accurated and, where necessary, kept up to date*

- *processed for a limited time*

Furthermore the data processor is expected to adopt appropriate measures in order to ensure the security of the data.

2.2.5 Consent

The GDPR confirms that the consent is required in order to process personal data. Consent must be freely given, specific, informed and unambiguous, and cannot be negotiated (e.g. where a service is provided only where a consent is granted by the data subject).

In particular, privacy policies and other documents provided to the data subjects must be written in a clear form, so that even a person without technical or legal expertise would understand the privacy implications of the processing.

The Regulation grants data subject the right to withdraw the provided consent in any moment. In any case, the data processor is expected to store the proof that an expressed consent has been provided.

2.2.6 Privacy by design and Privacy by default

Privacy by design may be defined as the outset of any product or process must comply with specific policies, procedures and systems

According to the privacy by default principle, data controller must implement mechanisms for ensuring that, by default, only the personal data which are necessary for each specific purpose of the processing are processed, and that they are not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of data and in terms of time of their storage.

2.2.7 Privacy Impact Assessment

As mentioned, the GDPR has assumed an accountability approach according to which data controllers are expected to make a preliminary check on the potential risks connected with the processing of personal data.

In this context, a basic role is given to the privacy impact assessment (PIA), which is one of the most important news introduced by the GDPR in the data protection scenario.

In any situation where a data processing may involve personal information, data controllers are expected to conduct a privacy risk assessment, together with the DPO, in order to ensure that such processing is compliant with the requirements of the GDPR. The PIA is due if the processing is "*likely to result in a high risk*" (such as, for instance, users profiling, processing of sensitive and judicial data).

The GDPR does not provide a complete list of the cases in which a processing is likely to result in a high risk, and the data controller is the one, together with the DPO, who has to evaluate these potential risks. The risks may be minimized by taking some technical and legal measures, such as: pseudonymization/anonymization of personal data; adoption of certifications; adhesion to codes of conduct; implementing privacy by design and privacy by default procedures.

In case of residual high risks, the data controller will have to contact the competent data protection authority for a prior consultation. In this case, the DPA will decide whether the data processing may expose data subject to relevant risks or not and authorize (or not) the processing.

2.2.8 Data breach

GDPR qualifies the data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If the data breach is likely to result in a high risk to the rights and freedoms of the natural person, the controller has the obligation to communicate it to the data subjects whose data may be involved in the data breach.

In case of data breach, the controller is expected to notify this event to the competent Data Protection Authority within 72 hours after having become aware of it. If it is not possible to comply with such deadline, the notification must explain the reasons for the delay.

Data processors, on their behalf, are expected to immediately report data breaches to data controllers.

Pursuant to article 33 of the GDPR, the notification should at least describe the following information:

a) the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) the likely consequences of the personal data breach;

d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

It should be noticed that in case of non-compliance, the administrative fines can be up to €10,000,000 or up to 2% of the total worldwide annual turnover of the preceding financial year. In the most severe cases of non-compliance, the administrative fines can be up to €20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year.

2.3 The ePrivacy Regulation

On January 10th 2017 the European Commission issued a Proposal for a Regulation on Privacy and Electronic Communications (hereinafter "the Regulation"), set to replace the ePrivacy Directive. The aim of the Commission is to reinforce trust and security in the Digital Single Market by updating the legal framework: this Regulation would have a significant and far-reaching implications for internet-based services and technologies.

Article 5 of the Regulation explicitly states that "*electronic communications shall be confidential, any interference by natural or legal person without the consent of the end users concerned shall be prohibited*".

Like the GDPR, the Proposal is a «*regulation*». The EU Commission, again, chose this instrument instead of a directive, since the Regulation applies in all EU countries without the need for any implementation. It also means that the text of the Regulation is the same for all the member States, which do not have the power to modify it in the course of the transposition, and this aims at harmonizing the data protection rules in all the EU countries, providing a legal instrument which is the same for all the entities which operate within the EU territory.

2.3.1 To whom it applies

The ePrivacy Directive only applies to traditional telecoms operators, while the ePrivacy Regulation would cover new providers of electronic communications services (such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, or Viber). The Regulation applies to the processing of electronic communications data processed in connection with the provision and the use of electronic communications services but also to information related to the terminal equipment of end user[2].

Similarly to the GDPR, with this regulation the EU Commission would extend the territorial scope of application to all providers of electronic communications services, including over-the-top service providers (OTTs) based outside EU. According to the Regulation, OTTs are the internet-based services enabling inter-personal communications (e.g., instant messaging, VOIP services, web-based email, IoT devices, machine-to-machine communications), which are currently not covered by the ePrivacy Directive 58/2002. Then, the Regulation expands the reach of European law to non-EU companies providing electronic communications services to, or processing data of, European individuals.

2.3.2 What is regulated by ePrivacy Regulation

Restrictions on the Use of Electronic Communications Data. The Regulation significantly limits the processing of electronic communications data to:

i. the content of the communications (e.g., text, voice, sound, images, videos)[3], and

ii. the metadata (e.g., location, date, time, duration, type of the communication)[4], please note that the term 'metadata' replaces the current definition of 'traffic data' under the current e-Privacy Directive.

Normally electronic communications data can only be processed as necessary to guarantee the transmission of the communication or to ensure the security of the communications. In addition, the Proposal allows the processing of metadata and the content of electronic communications in limited situations:

- Content of communications can be processed: for the sole purpose of providing a specific service to an end-user, if the end-user consent to the processing and if that processing is necessary to provide the service; or if all parties to the communication consent to the processing of the content for a specific purpose, given that this purpose could not be achieved by processing anonymous data and that the company complies the GDPR prior consultation requirement.
- Metadata can be processed: if the end-user concerned consents to the processing of metadata for specific purpose and provided that the purpose could not be achieved by processing anonymous data; if necessary to meet mandatory quality of service requirements; or if required for billing, calculating interconnection payments, detecting or stopping fraudulent or abusive use, or subscription to electronic communications services.

[2] Art. 2 of Proposal for a Regulation on Privacy and Electronic Communications

[3] Art. 4 paragraph 2 lett. c) of Proposal for a Regulation on Privacy and Electronic Communications

[4] Art. 4 paragraph 2 lett. d) of Proposal for a Regulation on Privacy and Electronic Communications

Cookie Law. The Proposal keeps the requirement to obtain prior informed consent for using cookies and similar technologies. The prior consent is not required if the use of such technologies is necessary for:

i. the sole purpose of carrying out the communication; or

ii. to provide an information society service[5] requested by the individuals.

It is worth noting that the Regulation simplifies the process by recognizing that the consent can be obtained via browser settings and by creating an exemption from the consent requirement for first party analytics.

Users' Terminal Equipment. The ePrivacy Regulation holds conditions for the collection of data emitted by users' terminal equipments[6] (MAC address, IMEI[7], IMSI[8]). Such data collection is only permitted to establish a connection; if users receive a clear and prominent notice that complies with the GDPR privacy notice requirements and explains the measures individuals can take to minimize or stop the data collection; and if appropriate security measures are in place. The goal is to cover the tracking of users' devices for services such as people-counting in defined areas, or providing personalized offers to individuals as they enter a store.

Direct e-Marketing Rules. The e-marketing provisions will be applicable to all communications means (e.g. automated phone calls, instant messaging application, social media messaging, SMS, MMS, Bluetooth, e-mails). Direct e-marketing to individuals requires prior informed consent (opt-in), unless communications are sent to existing customers regarding the company's own similar products or services and the customers receive means to opt-out at the time of data collection and in each marketing communication.

2.3.3 Final Remarks

The proposal is part of a much wider picture of interventions that the Commission is taking in order to ensure higher data protection.

The timing for the ePrivacy Regulation adoption remains uncertain, but it generally takes several months from the date of publication of a proposal. The Regulation was expected to be issued in a due time in order to enter into force together with the GDPR (from May 2018). However, such a time schedule has not been respected by the EU Commission, while the European Data Protection Board in its recent statement[9] on May 2018 calls for a swift implementation of the ePrivacy Regulation.

On 10 July 2018, the Council of the European Union has published a draft[10] of revisions to the proposed ePrivacy Regulation.

---

[5] Information society service means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (mainly online marketplace, online search engine, cloud computing)

[6] Art. 4 paragraph 2 lett. d) of Proposal for a Regulation on Privacy and Electronic Communications

[7] The International Mobile Equipment Identity or is a number, usually unique, to identify 3GPP AND IDEN mobile phones, as well as some satellite phones.

[8] The International Mobile Subscriber Identity or IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks.

[9] https://edpb.europa.eu/node/91

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT&from=EN

3 European and national legal frameworks on digital identity

Several European countries currently support the digital identity project as follow:

- Italy with the *Sistema Pubblico di Identità Digitale*,
- Austria with the *National Citizen Card*,
- France with *France Connect*,
- Spain with the *Documento Nacional de Identidad Electrónico*,
- Germany with the *German eID*,
- Luxembourg with the *Luxembourg National Identity Card*,
- Croatia with the *National Identification and Authentication System*,
- Belgium with the *FAS scheme*,
- Portugal with the *Cartão do Cidadão*.

In the following subsections, the eIDAS regulation as well as the current digital identity projects related to the PoSeID-on pilots countries are described.

3.1 Electronic Identification and Trust Service Regulation (the eIDAS Regulation)

The so-called eIDAS Regulation is a set of standards that aims to boost the user convenience, trust and confidence on the digital world while keeping pace with technological developments, promoting innovation and stimulating competition. It provides a regulatory environment for electronic identification, encouraging people to trust in electronic systems.

eIDAS compatibility and compliance ensures that businesses and citizens can use their own digital IDs to access public services in every European country that supports eIDAS. The regulation promotes the interoperability of public services across Europe, permitting to a user of a system provided by one member state to be able to access services from another member state (that operates with a different system) connecting through eIDAS.

3.2 The Digital Identity system adopted in Italy

The Digital Identity system adopted by the Italian government is called SPID and stands for Sistema Pubblico di Identità Digitale (Public System for Digital Identity).

Together with Germany, Italy was the first country to notify the European Commission about the governmental Digital Identity Project. The program, that aims to implement electronic interactions between businesses, citizens and public authorities, was introduced and is managed by the Agency for Digital Italy (AGID), and is compliant with the eIDAS Regulation.

SPID is an open system that allows public and private agencies – as long as they are accredited by AGID – to offer services of electronic identification for citizens and businesses. Italy has been the only European country, so far, to adopt a system of accreditation with the participation of private companies, so not entirely regulated by governmental authorities.

The providers of the identification services have to ensure a suitable procedure for the initial identification and have to implement a system of authentication for citizens. These service providers may be public or private organizations, on condition that they adhere to SPID.

SPID allows Italian citizens to access all online services of the Public Administration with a single Digital Identity (username and password) that can be used from computers, tablets and smartphones. Citizens can obtain SPID through an Identity (ID) Provider (the aforementioned private and public companies accredited by AGID) that will run a verification procedure to certify the user's identity. After the verification and confirmation of the applicant identity, a set of credentials is released and can be used in all websites (the aforementioned Service Providers).

Until now, the system has been used only for Public Administration's website, but the project foresees the utilization of SPID also for private companies' websites, as it may be useful when providing online bank or insurance services, for example.

Just a small number of projects for digital identity are based on authentication systems that do not involve the use of a Sim Card. Having a look at the projects so far notified, pre-notified and in development by European member states only Italy, France and Austria (with the mobile phone signature system) offer such an innovative solution.

3.3 The Digital Identity system adopted in Austria

Digital Identity system in Austria depends on the use of the National Citizen Card, provided with a Sim card (e-card). The citizen card token offers functions for identification and authentication and is the element that ensures that the user has solitary control when accessing applications. It is a form of electronic identification for people to be uniquely identified in the Internet environment.

However, the user can also access his/her digital identity using a mobile phone signature, in a Hardware Security Module (HSM), which is kept by the provider of the mobile phone signature in a secured environment in combination with the secret code of the signatory and the SMS-TAN that was sent to the signatory11.

The data stored in the citizen card include the user's first and last names, date of birth and the keys required for creating signatures.

- Mobile Phone Signature: it is the way to use a digital identity on a mobile phone. When accessing a national or European service that supports the Mobile Phone Signature, the citizen will be required to log in on the selected website. After typing his/her login data (login id and password) the citizen receives a code on his/her mobile phone or, if using a specific app, is able to use a QR code or fingerprint on the smartphone.
- Smart Card: requires a smart card with activated Citizen Card functionality and a smart-card reading device. People can insert the Citizen Card in the smart-card reading device and enter a password in order to be identified and recognized.

Both alternatives are used to create a legally valid signature in online procedures. These signatures are legally equivalent to handwriting signatures, so the mobile phone and the activated e-card became a virtual ID.

[11] https://www.digital.austria.gv.at/concept-citizen-card-and-mobile-phone-signature

The citizen card is frequently used for doing business with public authorities. However, the Austrian Government ensures that, with the mobile phone signature and the smart card, citizens are able to access different e-services from the public and private (e.g. e-banking) domain without need to manage numerous different login names and passwords.

The Austrian system is under development and was not yet notified to the European Commission.

Likewise the Italian project, Austria was the only country until this moment to present a project that enables the use of the digital id on a mobile device such as a smartphone.

3.4 The Digital Identity system adopted in France

France is developing a holistic identification and authentication system, called France Connect, to allow citizens, businesses and civil servants to access online services and to control how their data are exchanged. These Service Providers can be the public central administration, agencies for social services, local and regional authorities, but also private organizations such as industries, business innovators or non-profit operators.

Nowadays, French citizens who use online services, as the ones provided by the Ministry of Economics, Finance and Industry (DGFiP) or the Post Office (La Poste), are asked to create a personal account for each service. The role of France Connect is to federate these separate online identities and make them secure.

Hence, the ID Provider will be a website (as DGFiP or La Poste) that allows France Connect to identify and authenticate the user. The Service Provider, then, through a Data Provider, will access the France Connect database, which will pass to the Service Provider information and will authenticate the user. The ID Provider can be chosen from a list created by the French public administration and will automatically authenticate the user.

France Connect will act as a trusted party between administrations who support the protocol, so users will be able to authenticate using one of their existing administrative accounts.

The information of the user is collected by the ID Provider and then forwarded to France Connect, which creates a "Pivot ID" (Identité Pivot) that will be sent by France Connect to each Service Provider every time the user requests it.

Moreover, in a second step of the project, France has also the aim to exchange data between administrations. This means that administrations that have signed up to France Connect, with previous authorization by the user, will be able to transmit all the information needed for a particular administrative procedure without sending unnecessary data. In this cases, France Connect acts as a trusted intermediary, validating the user's ID before any data is exchanged12.

The French project has not yet been notified to the European Commission.

3.5 The Digital Identity system adopted in Spain

The Spanish mechanism to identify a digital identity is called Documento Nacional de Identidad Electrónico (DNIe). It certificates the digital identity with two different mechanisms: the authentication certificate and the signature certificate.

[12] https://joinup.ec.europa.eu/document/france-connect-id-federation-system-simplify-administrative-processes

Authentication Certificate: identifies the user when performing a telematics transaction. A PIN is associated with the authentication to ensure the identity of the user. Its main use is to generate identity confirmation and safe access to computer systems by establishing private and confidential connection with services providers. However, it does not guarantee to Service Providers users commitment with the operation or generated document.

Signature Certificate: allows the user to sign documents electronically with the same legal effects as a handwritten signature. Although, this certificate is not capable to generate identity confirmation and safe access to the computer system of Service Providers.

The DNIe system is based on a Sim Card, which contains the same data appearing at the card (personal data such as name and surname, Spanish id card number, date of birth, e-mail address, public key linked to the citizen; photography; digitalized signature and digitalized fingerprint), the authentication certificate and the electronic signature. The digital identification system is accessible with the use of a computer and a card reader.

The Spanish digital identity is not valid to legal persons and applies only to Spanish citizens living in the territory for more than six months.

Both mechanisms, therefore, guarantee the subscriber's identity and data protection while using a government-issued document combined with a PIN13. The Spanish government sustains that the DNIe will assist users to easily connect with governmental authorities or public and private companies, preventing citizens of queuing or moving around to issue official documents.

4 Conclusions

PoSeID-on aims to comply with the European legal framework on data protection, privacy and digital identity. This means that PoSeID-on will apply Data Protection by Design and by Default principles stated by the GDPR, meaning the following approach in the platform implementation:

- Data Protection as default setting;
- Data Protection embedded in the design of the platform;
- End-to-end security: full protection through the data lifecycle;
- Transparency of protection mechanisms;
- Maintaining user-centered focus.
- Data protection measures are switched on by default into the PoSeID-on platform, and not left to the user to activate.

Moreover, PoSeID-on will carefully provide access management applying the eIDAS Regulation to secure electronic identification and authentication to the dashboard.

PoSeID-on platform implementation presents thus some challenges that must be faced since the early stages of its design, to ensure data protection and respect of citizens fundamental rights. Those challenges will be carefully assessed in the following stages of the project, while conceiving the system architecture and implementing its components.

[13] http://firmaelectronica.gob.es/Home/en/Ciudadanos/DNI-Electronico.html