Impulse

Identity Management in PUbLic SErvices

D3.3 IMPULSE Method for ethical and legal assessment

Lead Author: Francesca Morpurgo (CEL)
Carmela Occhipinti (CEL)
With contributions from: Federico Pierucci (CEL), Luca Mattei (CEL)
Reviewer: Alicia Jiménez Gonzàlez, Nicholas Martin

Deliverable nature:	R
Dissemination level: (Confidentiality)	PU
Delivery date:	25-01-2023
Version:	1
Total number of pages:	42
Keywords:	Identity, Electronic Identity, Digital Identity, Identity Management, Deontological Approach, Value Sensitive Design, Self-Sovereignty, Privacy, Consent, GDPR, Data Ownership, Rights, Values, Biometric Identification, Ethics of Technology, Ethical Model, Accountability, Responsibility

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Executive summary

This deliverable aims to provide the assessment of the ethical and legal impacts and risks of the digital identity management on the society, and in particular of the Self-Sovereign model that is provided within the IMPULSE solution. In addition, it provides the assessment of biometrics and facial recognition technology adopted by IMPULSE, arising specific ethical concern. The present document aims to achieve the following different goals:

1. Provide a complete overview of the ethical and legal risks that new way of conceiving digital personal identity creates.
2. Offer a methodology that allows both theoretically and operationally to evaluate and provide countermeasure to those challenges.
3. Provide the assessment of the identity management approach and related technology adopted by IMPULSE.

To achieve this objective, a significant part of the scientific literature has been scanned and analysed, to analyse the identity management from a philosophical perspective and provide a preliminary assessment of the most significative social values associated to the identity concept. The results of such an initial assessment are then translated into risks for the human fundamental rights and interpreted in light of what has been done by the project in order to face them.

This document has been redacted trying to bridge different knowledge-sectors: from the more philosophical sides, it will present an analysis of the most relevant ethical approaches, that have been used for assessing the ethical risks. Accordingly, from the legal side, the legal risks have been assessed too. Then, different set of skills, expertise and techniques of social enquiry have been applied to the IMPULSE approach to the identity management as well as its software solution to assess their compliance on the relevant ethical principles and legal constraints.

Document information

Grant agreement No.	**101004459**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	https://www.impulse-h2020.eu/		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D3.3	**Title**	IMPULSE method for ethical and legal assessment
Work package	**Number**	WP3	**Title**	Multidisciplinary analysis of standards, legal and ethical implications
Task	**Number**	T3.3	**Title**	Implementation of a multi-stage method of assessment

Date of delivery	**Contractual**	M24	**Actual**	M
Status	version 0.2		☐Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)				
Responsible author	**Name**	Francesca Morpurgo, Carmela Occhipinti		
	Partner	CEL	**E-mail**	f.morpurgo@cyberethicslab.com

Summary (for dissemination)	*Description and application of a multi-stage method of ethical evaluation of IdM that combines the bottom-up approach of co-creation with the need for a universal vision of digital identity ethics in providing public services*
Keywords	*Identity, Electronic Identity, Digital Identity, Identity Management, Deontological Approach, Value Sensitive Design, Self-Sovereignty, Privacy, Consent, GDPR, Data Ownership, Human Rights, Values, Biometric Identification, Ethics of Technology, Ethical Model, Accountability, Responsibility*

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
25/02/2022	0.1	Federico Pierucci (CEL)	ToC
24/03/2022	0.2	Federico Pierucci (CEL), Luca Mattei (CEL)	ToC changes and section 1 & 2
15/12/2022	0.3	Francesca Morpurgo (CEL)	ToC changes and references
04/01/2023	0.4	Carmela Occhipinti (CEL)	Content and structure changes
10/01/2023	0.5	Francesca Morpurgo (CEL)	Content and structure changes
16/01/2023	0.6	Carmela Occhipinti (CEL)	Content revision
19/01/2023	0.7	Francesca Morpurgo (CEL)	Content changes
24/01/2023	0.8	Francesca Morpurgo (CEL)	Ready for the internal peer review

26/01/2023	0.9	Alicia Jimenez Gonzalez, Nicholas Martin	Peer Review
30/01/2023	1	Francesca Morpurgo	Final Version

Table of contents

List of tables

Abbreviations and acronyms

B-Based IdM: Blockchain-based Identity Management
B-Based IdM Systems: Blockchain Based Identity Management Systems
BC: Blockchain
DL: Distributed Ledgers
FIdM: Federated Identity Management
ICT: Information and Communication Technologies
IdM: Identity Management
IDP: Identity Provider
PoW: Proof of Work
RP: Relying Parties
SSI: Self-Sovereign Identity
SSIdMS: Self-Sovereign Identity Management Systems
SSO: Single Sign On
URI: Uniform Resource Identifier

1 Introduction

The aim of the IMPULSE project is to experiment with both a new technology and a new method of managing citizens' identity, a method based on the concept of Self-Sovereign Identity and that inscribes itself into the wider EU digital wallet project. As such, the IMPULSE project needs to be ethically assessed from both the perspective of the introduction of a new technology into a societal context, and of the management of the citizens' identity, with all its philosophical and practical consequences.

Consequently, the following two assessment levels have to be taken into account:

1. Philosophical and societal level: it should be noticed that the identity is both a "natural" right (it comes prior to its certification by the State) and a right deriving from the fact that the individual is inscribed into a social context regulated by rules and laws. From this twofold nature it derives that a way of providing and granting an identity to citizens must be evaluated both philosophically (what is identity? What are the ethical consequences of adopting an approach rather than another one when providing and certifying the citizens' identity?) and societally (what are the consequences of the introduction of a certain system of managing identity into a society? Are there any unseen consequences or aspects of it that should be considered when designing and then delivering a new identity management system into a society?).
2. Technological level: the IMPULSE technological solution needs to be assessed to verify if social values posed by the management of the digital identity have been handled by the IMPULSE technological solution.

To this extent, an IMPULSE tailored assessment method has been described (section 2) in five different steps as follows:

Step 1: Overview of Identity as a *moral concept*

Step 2: Identification of areas of impact

Step 3: Evaluation of risks

Step 4: Assessment

Step 5: Recommendations

Step 1 is discussed in detail in section 3 the main philosophical, ethical and legal questions emerging from the concept of identity and from the introduction of a form of digital identity based on the self-sovereign concept.

The second step is the topic of section 4, where philosophical and sociological challenges and questions connected to identity management have been depicted using two different approaches for two different purposes: the assessment of the technology design and the assessment of the technology itself.

Then, in section 5, the ethical and legal risks derived by the above-described social values are identified (step 3)5. Results from the co-creative workshops with stakeholders (D2.2 and D2.3) are here taken into account, to frame the framework that lies at the basis of the adopted system requirements.

The IMPULSE assessment (step 4) is finally carried out in section 6.

Step 5, i.e., recommendations for future implementation of digital identity services, have to be defined in conjunction with the feedback provided by the policy makers in T3.5 and of the outcomes of the IMPULSE pilots. Therefore, while the conclusion of the current document contains some hints on future recommendation, they will be completed only after the redaction of the second policy brief at the end of the project. They will then be part of deliverable *D3.7 Recommendations on standards, ethical, legal and privacy issues*, due at the end of the project lifetime.

We also briefly address the problem of the use inside the system of biometrics and facial recognition, indicating benefits, risks and possible mitigation actions. Further investigation will be performed in the next project months, in the final policy brief.

2 IMPULSE assessment method

The aim of this section is to illustrate the tailored method that has been conceived to assess the impact of the IMPULSE technological solution on relevant ethical principles and legal constraints, in order to promote its social acceptability by the society as a whole, in terms of to what extent the innovation brought by IMPULSE can improve people's lives.

To this extent, with the twofold aim of assessing the approach IMPULSE adopted to the identity management, as well as the design and implementation of the IMPULSE technological solution, a process based on the definition of social values and risks for the human fundamental rights has been depicted as follows:

Table 1: Document structure

Step 1: Identity as a *moral concept*	The first step consists on the explanation of the **identity as a *moral concept*** in general and in the context of the self-sovereign concept, adopted by IMPULSE.
Step 2: Identification of areas of impact	The second step is to define some **Areas of Ethical and Legal Impact of the identity management.** This will help define the scope of our risk and impact analysis, based on the review of the relevant scientific literature, the consortium expert judgement and the stakeholders' feedback.
Step 3: Evaluation of risks	The third step is to derive the **ethical** and **legal risks** that are associated with the Areas of Impact that are identified in the first step.
Step 4: Assessment	The fourth step consists on carrying out the **assessment** of the IMPULSE technological solution design and implementation through the defined approaches. In this section, also the facial recognition technology used by IMPULSE for the users to attest their identity will be assessed.
Step 5: Recommendations	The outcome of the activity carried out in this deliverable, combined with the results of the policy round tables (T3.5) and their outcomes in the form of policy briefs (*D.3.5*, *D3.6*), and of the IMPULSE pilots, will suggest recommendations based on the project lessons learned. They will be of input of deliverable *D3.7 Recommendations on standards, ethical, legal and privacy issues*, due at the end of the project lifetime.

2.1 IMPULSE assessment approach

The assessment of the ethical impacts (whether positive or negative) of a certain action, project, artifact or technology is indeed strictly dependant on the adopted approach. Suffice it to think, for instance, of the death penalty, that is considered abominable or acceptable depending on the moral values and principles the society adopts. Many different ethical theories and approaches have been developed by the philosophical reflection over the course of time. Among them, two different approaches in ethics of technology better fit with the twofold aim of assessing:

- the approach IMPULSE adopted to the identity management
- the design and implementation of the IMPULSE technological solution.

The two proposed approaches are here after described through an introductory explanation that should make it possible for both experts and non-experts in ethics and political philosophy to acquire some familiarity with the technical notions that are going to be employed in this deliverable. Since those definitions are taken as an aid to the reader (and not as an exhaustive description), they should provide a general, albeit accurate, illustration of the most relevant approaches in ethics of technology taken into account in the IMPULSE technology assessment.

- **Deontological approach:** The approach in which a certain ethical statement (either a prescription or a prohibition) has its *normative strength* in itself. No matter how certain beneficial consequences could stem from the violation of a prescription, in the deontological models of **ethics we are compelled to follow norms just for their intrinsic value**. An example of this would be the prescription "Lying is wrong". In the strongest and most notable formulation of the deontological position, made by Kant

(Williams 2005)[1], we cannot deviate from the actions that are prescribed by those statements for whatever reason, albeit intuitive, we could pose to this case. Less restrictive positions put instead their focus on intentional and situational elements for allowing a certain amount of flexibility. This approach allows to identify the ethical values that must be respected and incorporated into the design of any IDM solution, no matter what. Identifying these requirements is a very important component of an ethical and legal assessment because they represent constraints, the violation of which would compromise the ethical validity of the entire project. The question is whether the IMPULSE IDM solution as it is conceived and implemented is capable of respecting the identified requirements.

- **Value Sensitive design:** A family of theoretical and empirical approaches born to study the development of new technology from a *value-based* perspective. With value-based design we aim to capture **what are the fundamental values that are embedded in the process of designing technologies** (Friedman & al, 2013)[2]. In this approach, a multi-level method is presented, assessing the design process from a conceptual, empirical, and technical standpoint (Freidman & Hendry 2013)[3]. Value-sensitive design claims that some fundamental assumptions are constitutionally present in the design phase, and it aims to uncover them using a multifaceted methodology. This approach has been applied, giving valuable insights, on the problem of cookies and informed consent (Freidman et al 2000)[4]. This approach is particularly interesting for the development of a methodology of assessment of an identity management system, such as IMPULSE, because it is capable of highlighting both the hidden values that lie at the basis of certain design choices and the way these values and the resulting technology impact on the society and are impacted by it, in a sort of feedback loop circuit. The value sensitive design allows us to critically consider the way in which the core values we identify are then translated into design choices and what are the effects of these choices. To be noted that here also the design process matters: this approach implies a co-creative, participatory approach, that considers and reflects the needs of the stakeholders. Checking whether such an approach has been adopted will be part of the assessment process.

To be noted that the value sensitive design and the deontological approach are not two concurrent models but they can be instead seen as two steps of an evaluation process: the deontological approach is a philosophical model (that here will be inevitably simplified) whose aim is to establish some normative values and principles that any action must comply with to be defined "ethical"; the value sensitive design approach is not a philosophical model but a way of approaching design and in particular the design of technology, and can be used with whatever system of values or ethical model, since it deals with the way the design choices reflect and respect the values characterizing the reference ethical model. So, they complement each other.

In order to assess what are the implications of IMPULSE in terms of risks on the human fundamental rights, first the deontological model will be applied in the following sections to identify ethical, social and legal values and constraints applicable to the IMPULSE identity management approach.

Then, adopting a value sensitive design approach combined with the co-creative approach described in D2.2 and D2.3, the method will assess whether and how the identified values and constraints have an influence on design choices and if the actual implementation of the IMPULSE solution satisfies them.

[1] Flathman, R. (2006). In the Beginning Was the Deed: Realism and Moralism in Political Argument. Perspectives on Politics, 4(2), 375-376. doi:10.1017/S1537592706320270

[2] Friedman, B., Kahn, P.H., Borning, A., Huldtgren, A. (2013). Value Sensitive Design and Information Systems. In: Doorn, N., Schuurbiers, D., van de Poel, I., Gorman, M. (eds) Early engagement and new technologies: Opening up the laboratory. Philosophy of Engineering and Technology, vol 16. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-7844-3_4

[3] Hendry, D.G., Friedman, B. & Ballard, S. Value sensitive design as a formative framework. Ethics Inf Technol 23, 39–44 (2021). https://doi.org/10.1007/s10676-021-09579-x

[4] Friedman, B., Kahn, P., & Borning, A. (2002). Value sensitive design: Theory and methods. University of Washington technical report, 2, 12.

3 Identity as a *moral concept*

The first step of the applied method consists on an overview of the identity concept at philosophical and legal level that will pave the ground for the successive assessment steps.

Identity is a complex construct that historically is strongly intertwined with the need for control over the individual by the state and with people's rights and construction of the self by means of a set of relational structures.

On the one hand, a unique identity is necessary to identify people as subjects of certain rights and/or obligations, on the other hand, being tied to a certain identity may enable to access certain rights or privileges or to being excluded and discriminated against. Also, there is the problem of the continuity of identity through the years: can identity remain the same while the person to whom it is attached changes? Does the individual have the right to have an identity that fully mirrors the way he/she feels about him/herself? As Manders-Huits (2010)[5] points out there is the risk to fall into a form of "practical" reductionism where the individual is forced to accept a flattening of his/her identity to an "administrative" notion of it that doesn't reflect the full complexity of one's vision of himself.

Ishmahev and Stokkink (2020)[6] highlight how difficult it is from a conceptual and philosophical point of view "tame" all the complexities connected to the concept of identity to obtain a viable and "usable" definition that can be adopted as the ethical basis of an identity management system, be it digital or not. Any attempt to simplify the way to approach "identity", as outlined in (Manders-Huits and Hoven, 2008), inevitably impacts on fundamental moral aspects of human life such as autonomy, self-determination, and self-identification.

From the analysis of Ishmahev and Stokkink (2020) it definitely emerges a tension between an approach to identity management focused on the individual and his/her rights and the society. To exemplify this concept, they use the case of the Chinese "Social Credit System" (SCS) where a social scoring is introduced with the moral justification of identifying and isolating the "bad elements" from the society, something that in this view would result in a clear advantage for the society as a whole (at the expense of the rights and the well-being of the individual).

This is an interesting example because it makes immediately visible one aspect that is central to our analysis: **the value system that is underlying to a certain society in a certain historical moment is a fundamental element of the construction of an identity management system**, both to understand the reason why it has been developed in a certain way and to introduce the necessary corrections – if needed.

Individual values like self-determination, moral autonomy, rights to privacy and to full control over one's data conflict in some way with communitarian values like accountability, obligations towards others, responsibility for one's actions.

When an identity management system is designed, a choice is inevitably made to privilege some values over others. In the course of this deliverable, we are going to highlight which choice was made in the design of the IMPULSE eID system and if the system that has been developed is compliant with that choice.

The above is true of any system of identity management but, as Zwitter et al (2020)[7] show in their paper, digital identity brings forward an entire new set of problems, beginning from that of the fragmentation of identity: while usually we have only one ID card, on the digital space each individual possesses more than one digital identity issued by different providers (what Allen (2016) calls "balkanization of identity"), each one of them controlled by a different issuer and with different attributes (are your job, your education, your interests, part of your "identity"?) that all together compose the identity of the individual. Should we aim to a singular persistent identity (and impose it)?

[5] Manders-Huits, N. (2010). Practical versus moral identities in identity management. Ethics Information Technol. 12, 43–55. doi: 10.1007/s10676-010-9216-8

[6] Ishmaev Georgy, Stokkink Quinten, Identity Management Systems: Singular Identities and Multiple Moral Issues, Frontiers in Blockchain Vol 3 2020, https://www.frontiersin.org/articles/10.3389/fbloc.2020.00015, DOI=10.3389/fbloc.2020.00015

[7] Zwitter, Andrej and Gstrein, Oskar Josef and Yap, Evan, Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual (March 4, 2020). Front. Blockchain, 28 May 2020 | https://doi.org/10.3389/fbloc.2020.00026, Available at SSRN: https://ssrn.com/abstract=3454513 or http://dx.doi.org/10.2139/ssrn.3454513

While traditional identity certification is a necessity (dictated by power relations and governance structures), digital identity has become a "basic infrastructural service" (Zwitter et al 2020) that follows different rules and obligations and that is needed to access certain services, not necessarily public and not necessarily basic.

Since digital identity is "free" (each provider establishes its own rules) and fragmentated, the way it is shaped and managed is not neutral. For instance, as outlined by (Lessig, 2006)[8], we know that the ways in which online communities are structured and the ways in which identity is managed inside them may change the moral capabilities of the agents (the communities' members).

How much an individual can be considered accountable over his/her action, how much anonymity and freedom can be favoured over public responsibility and liability, Lessig observes, is a political and moral choice that is to be made when it comes to the design of the network capabilities and participation rules.

There are roughly three main possible models of identity management: centralized, federated and decentralized. As defined in *D5.1 IMPULSE Technology Block V1*, **IMPULSE provides a decentralized eID solution based in the SSI identity model**.

3.1 The EU approach to the electronic identity

The basis for cross-border electronic identification, authentication and website certification within the EU was provided for the first time in Europe with the 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation or eIDAS). The regulation mainly focuses on cross- border access to public services and is based on national eID systems that follow varying standards.

Then, during the 16 September 2020 discourse on the State of the Union, the European Commission's ambition to deliver a secure and trusted digital identity to all EU citizens was announced. In that occasion the President of the European Commission announced that:

"We want a set of rules that puts people at the centre. (…) This includes control over our personal data, which we still have far too rarely today. Every time an app or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used".

At the urging of the increased need of accessing to public and private services highlighted by the pandemic, on 3 June 2021, the Commission put forward a proposal building on the eIDAS framework, with the aim of giving at least 80 % of citizens the possibility to use a digital identity to access key public services by 2030 and to do so across EU borders. The aim is to allow citizens to identify and authenticate themselves online via their **European Digital Identity Wallet (EU DIW)**. A legislative proposal for a European DIW was submitted, as part of the revision to the eIDAS Regulation, known as eIDAS 2, that is still under discussion by the EU institutions.

In parallel, the Commission adopted a recommendation to design a toolbox supporting the framework so as to avoid fragmentation and barriers due to diverging standards.

Contextually, an impact assessment report was released by the Commission Staff.[9] In this document a definition of digital identity is given[10] and a set of 4 core objectives is set up:

[8] Lessig, L. (2006). Code and Other Laws of Cyberspace, Version 2.0. New York: Basic Books.

[9] IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity - Available at: https://ec.europa.eu/newsroom/dae/redirection/document/76618

[10] "A digital identity is a digital representation of a natural or legal person. It lets you prove who you are during interactions and transactions. Attributes contain information about a subject. This can include details such as your legal name or date of birth, as well as details from other organisations, such as your professional qualifications, bank balance or medical history. Today, it is considered that digital identities are also comprised of such characteristics or attributes related to an individual, an organisation or an electronic device. The information contained in a digital identity allows for the authentication of a user or the presentation of his/her digital attributes, giving him/her access to public or private services online or offline.

1. Provide access to trusted and secure digital identity solutions that can be used cross borders, meeting user expectations and market demand.
2. Ensure that public and private services can rely on trusted and secure digital identity solutions across borders
3. Provide citizens full control of their personal data and assure their security when using digital identity solutions
4. Ensure equal conditions for the provision of qualified trust services in the EU and their acceptance

with the overarching objective on ensuring "*the proper functioning of the internal market, particularly in relation to the provision and use of cross-border and cross-sector public and private services relying on the availability and use of highly secure and trustworthy electronic identity solutions*".

As per the impacts on social inclusion and fundamental rights, the EU digital wallet - developed as a system that "*would empower users to securely share data related to their identity to public and private online service providers through their mobile device and allow them to control their own personal data in a user centric way […] allowing the user to integrate a national eID and various credentials obtained from private and public providers) and link them to specific identification and authentication services*" (ibidem p. 45) - should promote better compliance with the Charter of Fundamental Rights of the European Union[11] and in particular with the following human rights:

- Freedoms, in particular for what pertains to personal data protection, security and transparency of processing, reduced risk of ID theft
- Equality, because an easier access to public and private services would promote the inclusion of people with disabilities, low literacy, or that in any case may experience barriers in accessing the services in person
- Solidarity, through easier access to online services
- Inclusion, making it easier the access to core services like healthcare, instruction, social assistance also to people who experience difficulties in accessing them in person (for instance people living in rural areas)
- Engagement and participation, through an easier and more secure access to digital services online (for instance voting could be a lot easier if it could be accessed online)
- Freedom of movement and of residence, increasing opportunities to live, work and access services across EU without the constraint of the national borders and identification.

If we confront this set of values with the list of aims and values of the European Union[12], we can appreciate how this project complies with some of the fundamental aims of the European Union as laid out in the Lisbon Treaty[13].

Therefore, we can appreciate how the model of digital identity to which the EU aims is strongly oriented towards the full protection and promotion of the individual rights of the people, in particular for what pertains to the personal data protection and management, but also to the matter of the individual access to services and to the freedom of movement. Also the fact that identity should not be considered only in a strictly "administrative" way (in this recognizing that an individual possesses an identity even if and when this identity

The overall objective is to enable citizens and businesses to prove who they are or to prove their attributes/characteristics, without needing physical documents. What is emerging in the market today is a new environment where the focus has shifted from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities. […] A digital identity system that does not allow a seamless link with attributes and credentials is therefore no longer addressing current societal demands due to digitisation." IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity Pag. 11

[11] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT

[12] Accessible at https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en

[13] Accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016ME/TXT&from=EN#d1e79-47-1

is not certified by the State14, trivially when he/she crosses the borders) and that attached to it there should be (and should be manageable) also attributes like education, qualifications, hobbies, employment, etc. is stressed out, going towards the model of multiple, albeit reconcilable identities, changing over time and that the user can completely control. Finally, the need for trustability of the model is strongly emphasized.

The previously described model fully lies in the field of the so-called **Self Sovereign approach** to identity management, that we'll examine more closely in the section below as the approach **adopted by IMPULSE**.

3.2 The Self Sovereign model of Identity management

Considering the legal domain, the identity can be shaped by a number of individual rights that states are obligated to offer to individuals, notably in the human rights arena (legal determinacy).

Furthermore, issues of material and immaterial commodities ownership eventually emphasize **the problem of data ownership**, which may be critical.

According to Zwitter (Zwitter & Al 2021)[15], there is a spectrum in which different positions on identity are distributed between individualistic understandings of identity and relational understandings.

- **An individual-based definition of the digital** identity is mostly understandable in naturalistic terms. A possessor of an identity is mostly defined by the fact that a digital identity is the projection of some real attributes of an individual, that are transferred over the web. This is aided also by a means of identification that is founded upon some natural properties of the individual (either by finger-print or face-recognition).

  The **Self Sovereign** model expresses this model. The features that define it, given that the individual is the sole owner and controller of its credentials (Control), are usually identified by some natural properties, such as biometrical identifiers (Naturalism), the user is mandated to be always the same (Uniqueness), and it's not separated by his data (Wholeness). The uniqueness of the individuals is issued by their existence itself in a society, and given the fact that they possess an identity, it is in their natural right to have a digital one that has a biunivocal correspondence with the physical one. Furthermore, we observe an implosion of different online personas into one, because there is just one possible actor in this model. It fosters autonomy, albeit requiring some adaptation and some awareness from the user/citizen. In terms of identity, the user needs to be both unique (meaning that no two people should have the same identifier) and singular (meaning that no individual should have more than one identifier in the same domain). (Wang & De Filippi, 2020)[16]

- **A relational-based definition**, conversely, is mostly to be defined in constructivist terms. The strongest formulation of this position is the view that states that the identity is shaped by social structure, and the uniqueness of this notion of identity is attributed to the fact that there is a relation towards another part, where the identity is given only because of this relation. What is more, individuals can have multiple identity of this sort, seeing an explosion of online different personas that someone can relate to. This means that a value that we can assess here is Distinctiveness that is opposed to Uniqueness.

  The **Centralized Identity** model share those type of values: Individuals possess multiple accounts on different providers (Distinctiveness), are defined solely by arbitrary and abstract properties, such as Username and Password (Constructivism), and are not the owner of their data (Dividedness). This is mainly a network of actors that are provided with a set of services offered by external providers. It fosters heteronomy and allows for an easier to understand and ready-made service for the user/citizen.

[14] In the most extreme way of viewing it, "must emit directly from an individual human life, and not from within an administrative mechanism created by, for, as abstractions of individual human activities, and must remain amenable in design and intent directly by individual humans with original source authority", Loffreto, Devon. 2016. "Self-Sovereign Identity". The Moxy Tongue.https://www.moxytongue.com/2016/02/self-sovereign-identity.html

[15] Zwitter, Andrej and Gstrein, Oskar Josef, Editorial: Identity and Privacy Governance (August 06, 2021). Frontiers in Blockchain 2021, Available at SSRN: https://ssrn.com/abstract=3906511

[16] Wang, Fennie and De Filippi, Primavera, Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion (January 23, 2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, in Frontiers in Blockchain (Special Issue on Identity and Privacy Governance), 2020, Available at SSRN: https://ssrn.com/abstract=3524367

The **federated identity model** shows a mix of those two models, and it is represented by the possibility of using different services on the internet thanks to a federation (such as Google or Facebook) that guarantee the identity of the user.

The Self-Sovereign Identity model - based on the Decentralized Identity paradigm - is the one adopted by the IMPULSE technology solution.

The term sovereignty has a long history in political debate, being one of the central elements of modern political philosophy. The notion of Self-Sovereign Identity lends itself to some possible conceptual misunderstandings that arise from the history of the term, which traditionally has political and state connotations. Usually, within the literature, the term sovereign is referred to a state or a power figure: as far as the state is concerned, a state is sovereign if and only if it possesses the right to monopolize certain exercises of power concerning its territory and citizens[17].

The notion of sovereignty is generally predicated on objects and concepts of a political nature, applying it to the concept of identity was an innovation by Allen[18] that introduced it in the field of digital Identity Management.

The philosophical and ethical principles that underlies Self Sovereignty are founded on the tenet that the individuals are sovereign over their identity, and there is a new understanding of the power balance between the different part of the network (Preukschat e Reed 2021)[19]. Its revolutionary concept, according to Allen (2016)[20]is in the fact that:

"*Rather than just advocating that users be at the centre of the identity process, self-sovereign identity requires that users be the rulers of their own identity*".

There are some fundamental values that we are going to define concerning the notion of Sovereignty (Ishmaev, 2021)[21]: in the Self Sovereign model, the user is the sole owner of its data (ownership), the control is given by a natural right (self-determination) and is not granted from another individual or institution, it is recognized upon the identification of some natural properties that entitle the citizens automatically on their digital identity. The citizens are the possessor of these properties (singularity) and they are the only entity identified by it (unicity). Regarding the identity management aspect, Sovereignty is considered to be the ability to share verified credentials preferring minimal data disclosure**,** where the individuals exercise their control over identity relevant private data (Ishmaev, 2021, p. 242).

The self-sovereign identity paradigm founds its roots on a human-rights based notion in which an individual, that is *de facto* the possessor of certain distinctive features (since, being oneself, he is different from everybody else) is de iure possessor of an identity (Wang & De Filippi, 2020)[22]. How this notion can be fully grasped is using the concept of Sovereign Source of Authority: the claim for automatic recognition of an identity that is automatically guaranteed before any intervention of a nationally or internationally politically sovereign structure.

In this position it is strongly criticized the fact that the State (or another source of authority) may be the unique issuer and certifier of individuals' identity. Identity finds its roots in the fundamental rights and in the existence of the individual and not on a third entity that issues and/or certifies it (to formulate it in Allen's (2016) words, "I think therefore I am" as opposed to "I think, but I am not"):

[17] Stilz, Anna, 'Introduction: The Normative Bases for Territorial Sovereignty', Territorial Sovereignty: A Philosophical Exploration, Oxford Political Theory (Oxford, 2019; online edn, Oxford Academic, 24 Oct. 2019), https://doi.org/10.1093/oso/9780198833536.003.0001

[18] Allen, C. The Path to Self-Sovereign Identity. 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[19] Preukschat A, Reed D (2021) Why the internet is missing an identity layer – and why SSI can finally provide one. In: Preukschat A, Reed D (eds) Self-sovereign identity: decentralized digital identity and verifiable credentials. Manning, New York

[20] Allen, C. The Path to Self-Sovereign Identity. 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[21] Ishmaev G. Sovereignty, privacy, and ethics in blockchain-based identity management systems. Ethics Inf Technol. 2021;23(3):239-252. doi: 10.1007/s10676-020-09563-x. Epub 2020 Nov 30. PMID: 33281497; PMCID: PMC7701220.

[22] Wang, Fennie and De Filippi, Primavera, Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion (January 23, 2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, in Frontiers in Blockchain (Special Issue on Identity and Privacy Governance), 2020, Available at SSRN: https://ssrn.com/abstract=3524367

"*There is a natural conflict inherent in this approach to data administration via identity. The act of "registration" implies that an administration process controlled by Society is required for "identity" to exist. This approach contrives Society as the owner of "identity", and the Individual as the outcome of socio-economic administration. Within any Society, Individuals have an established Right to an "identity", and to all of the benefits and responsibilities of some form of "Nationally Sovereign Structure" of governance and administration. Sovereign Source Authority (SSA) refers to the actual default design parameter of Human identity, prior to the "registration" process used to inaugurate participation in Society. Currently, the administrative act of "registering new (baby) identities" eliminates SSA and replaces this default structural data model with a National administrative point of origin. There is a natural conflict inherent in this approach to data administration via identity. The act of "registration" implies that an administration process controlled by Society is required for "identity" to exist. This approach contrives Society as the owner of "identity", and the Individual as the outcome of socio-economic administration. This violates common-sense and the nature of Human Rights.*"[23]

[23] Loffreto, Devon. 2012. "What is 'Sovereign Source Authority'?" The Moxy Tongue. http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

4 Areas of Ethical and Legal Impact of the identity management

This is the second step of the IMPULSE assessment method (section 2). It finds its roots in the preliminary short outline of the main philosophical, ethical and legal questions emerging from the concept of identity and from the introduction of a form of digital identity illustrated in the previous section (section 3), demonstrating that **digital identity management technologies, such as the technology developed by IMPULSE, pose certain concerns and risks.**

For instance, the sovereignty, the control and the traceability over all the personal data may be (depending on the ethical approach we decide to adopt) considered a core value that inform and shape our decisions in conceiving, designing and deploying certain models of IDM. This in turn could lead to certain decisions regarding the identity management approach to adopt and the respective implementation.

Clarifying what are the relevant social values and legal constraints is the preliminary step to identify those risks. Moving from the theoretical analysis we made in the preceding section regarding the values and principles that lay at the basis of any approach to identity management, this section will **extract the IMPULSE theoretical guidelines (namely the values and principles that we identified as lying at the basis of the IMPULSE approach to digital identity) allowing to treat the concept of identity as a *moral concept***, and to assess their adoption by applying the assessment approach outlined in section 2.1.

4.1 Identity management from a deontological perspective

In a deontological perspective, the reason to choose one or more principles for action can be found in a lexicographic index of principles that needs to be respected in order to maintain the *procedural* and the *substantive* justice of a certain social organization. When it comes to digital identity and digital identity management, the approach to be adopted to ethically justify the choices that are made is the same: **identifying and choosing a set of foundational principles from the ethical and the legal standpoint**.

The values and constraints we will identify under the deontological model will then be used to act as a value system basis for the value sensitive design analysis, that as it's widely known is agnostic towards the effectively adopted values, the matter being checking whether the design choices have been respectful of those values.

Since **at the core of the IMPULSE eID approach there is the Self-Sovereign Identity (SSI)**, the following subsections will examine it against the wider landscape of the EU approach to digital identity and in general against the aims and values of the European Union[24], as well as against the requirements gathered by IMPULSE stakeholders. We will thus have a set of values on the digital identity management.

4.1.1 The Sovereignty model values

The following table shows a set of values **that are considered to be mandatory in the context of a self-sovereign approach to identity management.**

Those principles are formulated as *rights* and *requirements* that ethically ground the choice regarding eID.

In the first table we placed the principles formulated in the famous blog post called "The Path to Self-Sovereign Identity" of one of the founding fathers of the Self-Sovereign Identity, Christopher Allen[25], divided in three main aspects: User-related, Data-related, Architecture-related. The post illustrates Allen's vision on how the ability of digital identity might be enhanced to enable trust while preserving individual privacy, in the so called self-sovereign identity.

Table 2: Sovereignty model values

Principle	Brief Description	Description

[24] https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en
[25] Allen, C. The Path to Self-Sovereign Identity. 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

	User-related	
Existence	Users must have an independent existence	Any Self-Sovereign Identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.
Persistence	Identities must be long-lived	Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.
Protection	The rights of users must be protected	When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.
Consent	Users must agree to the use of their identity	Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.
	Data-related	
Control	Users must be in control of their identities	Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This doesn't mean that a user controls all of the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.
Access	Users must have access to their own data	A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.

Minimalization	Disclosure of claims must be minimised	When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatability is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.
	Architecture-related	
Transparency	Systems and algorithms must be transparent	The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.
Portability	Information and services about identity must be transportable	Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear — and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity no matter what, and can also improve an identity's persistence over time.
Interoperability	Identities should be as widely usable as possible	Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.

Those requirements relate to the following set of values:

Table 3: SSI model values

Value	Description	Principle
Wholeness	The user is not separated by his data	Existence, Persistence, Protection
Autonomy	The user must be central to the administration of identity	Control, Access, Minimisation, Consent
Shareability	The user must be able to decide to share an identity from one service to another	Transparency, Portability, Interoperability

4.1.2 Analysis of Allen's principles in the light of the GDPR

The GDPR is the most important European regulation when it comes to the privacy and data protection of natural persons. In order to show how Self-Sovereign Identity (the conceptual architecture in the IMPULSE

solution) is ethically compliant with the GDPR, we will now conduct a comparison between the principles stated by Allen in its foundational article and the GDPR's most fundamentals notions:

Table 4: SSI values in the light of the GDPR

Existence	(**Art. 1**. *Subject-matter and objectives*) The GDPR specifies that is appliable to natural persons. We should here refer to the notion of "Data Protection by Design": From the sole notion that a certain person exists in the EU territory, regarding the fact that their data are processed in Europe or not (**Art 3**. *Territorial Scope*), *"GDPR makes encryption a requirement for compliance by highlighting it as a suitable measure for data protection.*"
Control	The owner of the credentials is considered to be the first controller of the credentials, being able to fully decide when, where and how data should be processed. However, for accessing the services provided by different providers, the GDPR offers the possibility to lawfully give a portion of that sovereignty, namely the capacity to process and control the data, to the figures of the Controller and the Processer (**Art 24., Art 28**). Nonetheless, all the parties other than the Data subject needs to respect all the rights stated in the **Chapter 3** (Art. 12-22).
Access	The paradigm shift of the self-sovereign identity is aimed to empower the data subject, making them constantly aware of the operation on its data. The data subjects need to be constantly informed whether their data are being accessed. In the GDPR this principle is clearly stated in the **Art 15.**, that we are going to quote verbatim: *"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:* 1. *the purposes of the processing;* 2. *the categories of personal data concerned;* 3. *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;* 4. *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;"*
Transparency	The **purposes (Art 5) of the data processing** should appear clear and intelligible for the data subject. This can be ensured providing all the appropriate and necessary information to data subjects to exercise their rights, to data controllers to evaluate their processors, and to Data Protection Authorities to monitor according to responsibilities. The technology solutions, and their relative **data models**, thus should ensure that a data subject might get easily access, at any time also after the start of the data processing operations, to that information. For the sake of clarity, it should be noted that all that information should be made available to the data subjects in a clear and intelligible way.
Consent	**Art 7**. *"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data".*
Minimalization/ Minimisation	Differently from Allen, where the notion of **minimization** applies to the disclosures of claims (attributes that are to be verified), the idea of **minimisation** applies to amount of personal data that can be rightfully processed according to the **art. 5**: *"Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)".*
Portability	**Art. 20** *"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have transmit those data to another controller without hindrance from the controller to which the personal data have been provided."*

Protection	**Art 25.1** *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."*

The violation of those features and an approach that is not sufficiently careful in protecting personal data and guaranteeing the owner to be constantly in control of their data, may yield to negative outcomes regarding privacy protection. What is more, a lack of clarity in the definition of the consent form might produce, from the data subject side, an unwarranted assent to a process that the subject is not fully aware of.

4.2 Identity management from a value sensitive design perspective

Having outlined the core aims and values that – in a deontological perspective – lie at the basis of the IMPULSE model of identity management, we are now going to identify what kind of impact these values have on the project.

As mentioned in section 2.1 the analysis will be done staying into a value sensitive design perspective so as to highlight and understand the relationship between the design choices adopted into the project and the identified normative values.

The starting assumption is that technology is not agnostic towards certain social relationships, power and trust structures that are present in the community in which it is used and by which it is conceived and developed.

On the contrary:

"Technology is human behaviour that transforms society and transforms the environment. Design is the cornerstone of technology. It is how we solve our problems, fulfil our needs, shape our world, change the future, and create new problems. From extraction to disposal in the life-cycle of a product, the design process is where we make the most important decisions; the decisions that determine most of the final product cost, and the decisions that determine most of the ethical costs and benefits. It is quintessentially an ethical process." (Devon & De Poel 2004)[26]

Therefore, the following section adds to the assessment of the project identity management approach the assessment of the technological solution that concretises it, with the aim of effectively analysing the complex relationships between values and their incorporations into objects or technologies.

In other words, the ultimate aim is here to **understand how certain set of values and certain assumptions enter into the design of the technologies we wish to assess in terms of requirements**. **Step 3 of the assessment methodology will then transform these requirements into risks, while step 4 will verify if and how the designed technical solution manages to cope with them.**

Value sensitive design takes an interactional stance on the problem of how technology shapes (and is shaped) by the society. For interactional stance we mean that:

"Unlike approaches that lean toward technological determinism or social determinism, interactional theories such as value sensitive design posit that human beings acting as individuals, organizations, or societies shape the tools and technologies they design and implement, those tools and technologies shape human experience and society" (Friedman & Khan, 2003)[27].

Within sociotechnical systems, the values that are imbued in the design of certain technologies affect and shape certain behaviours of a society. What is more, in a **feedback loop mechanism**, the society itself modifies what spectrum of technologies are acceptable and what values concur to enter into a design process. The philosophical elements that underlie the development of certain technologies are sometimes hard to pin because they become embedded in them.

[26] Devon, R.E. and Ibo van de Poel. "Design Ethics: The Social Ethics Paradigm*." International Journal of Engineering Education 20 (2004): 461-469.
[27] Friedman, B., Kahn, P.H., Borning, A., & Huldtgren, A. (2020). Value Sensitive Design and Information Systems. The Ethics of Information Technologies.

A paradigmatic example of this phenomenon could be the debate between proprietary, open-source, and free software. According to Richard Stallman (2002)[28], a well-known voice in the free software community, there are four fundamental freedoms with which every program has to comply:

- The freedom to run the program as you wish, for any purpose (freedom 0).
- The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help others (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

We can observe that, under those conditions, **freedom** is considered such a fundamental value that needs to be present in all the possible instances of use of technology, both from an individual and from a community perspective. **Freedom in the design process is preserved also in the distribution moment, in which the software is shared among users**. On the other side of the spectrum, proprietary software does not allow the user to own the program, but just the licence, hide the access to the source code and usually forbid the user to either distribute and modify the program on his/own will[29] .

Both positions express different internal value configurations, which leverage different demands from a user group but also different considerations and effects on the social sphere. The juxtaposition of these two sets of values occurs at the moment when there are fundamental conflicts about **what guidelines to follow when a certain technology is conceived**, and its specifications are defined. Thus, the social effects and resonance on the user audience has different effects, relative to what the structures of this audience are.

Another example that has been studied in the area of value sensitive design is that of cookie management and informed consent (Friedman & Al 2000)[30]. In a nutshell, the term "**informed**" refers to both disclosure and comprehension.

- The term "**disclosure**" refers to delivering factual information regarding the rewards and risks associated with the action under consideration. The individual's accurate understanding of what is being presented is referred to as comprehension.
- The concept of "**consent**," on the other hand, incorporates voluntariness, comprehension, and agreement. The term "voluntarism" refers to the absence of control or coercion in the action. Competence is defined as having the mental, emotional, and physical capacities required to give informed consent.

A reasonable opportunity to accept or deny participation is referred to as **agreement**. Furthermore, the agreement should be continuous, meaning that the participant should be allowed to leave the engagement at any point.

From the examples above we can see that hidden in apparently neutral design choices (“do I place this button on this page”?) there may be profound and critical ethical values and aspects that strongly influence the product design and development and once made may in turn have a profound effect on society. To resume the first example, that of the free software, once a design choice is made (software must be free) and the product is released and used, this choice may influence the society transmitting the values it is imbued with, that become stronger and more accepted than before (the free access to knowledge and to instruments like software).

This is true also of IDM systems, and in particular of the approach adopted by IMPULSE (blockchain based Self-Sovereign Identity). So now the hidden values and choices underlying the system chosen by IMPULSE to manage digital identities of citizens will be picked out, to examine the process that brought to certain design choices and also to assess the potential impact that these choices may have on society.

[28] Stallman, Richard: Free Software, Free Society: Selected Essays of Richard M. Stallman (Boston: GNU Press, 2002), ed. by Joshua Gay, contrib. by Lawrence Lessig

[29] Richard Stallman, The Gnu Project. Available at https://www.gnu.org/gnu/thegnuproject.en.html

[30] Friedman, B., Millett, L., and Felten, E. (2000). Informed Consent Online: A Conceptual Model and Design Principles. University of Washington Computer Science & Engineering Technical Report 00–12–2

In section 4, the values that constitute the ethical baseline of the EU (generally and from the GDPR point of view) and of the IMPULSE approach to digital identity have been illustrated. The value sensitive design approach, once understood who are the stakeholders of a certain technology, works on the basis of the reconnaissance of the stakeholders' values into the design choices. But – as some critics point out[31], a more normative approach will be necessary, to avoid to incur in a form of subjectivism or of moral relativism, namely that each system of values would do. Also, there is the problem of possibly conflicting values, that into an ethically agnostic system would not be possible to reconcile.

For this reason, in the context of the IMPULSE project, from the one hand requirements have been defined adopting a value sensitive design stance (working bottom-up with **stakeholder groups** and eliciting the values and the requirements that should be embedded into the developed system, identified in deliverable D2.2) and they were assumed as the ethical framework of the IMPULSE project. From the other hand, as we saw in the preceding sections, also more **general and background normative values** have been identified, that act as an ethical and legal set of reference.

As per the high-level requirements that came out of the co-creation workshops, these are: technical robustness, trust, usability and user friendliness, accessibility and inclusion by design, security, compliance to legal regulations, technical, and ethical standards. Project deliverables D2.2 and D2.3 report the complete list of requirements as well as the description of the co-creative definition of them. In the following table we'll sum up the values that emerged from the consultation with the IMPULSE stakeholders, with the aim – in the next section – of transforming them into risks and assessing whether they have been mitigated. However, it must be noted that an effort and a commitment has already been made to embed the requirements below into the system's requirement, as per the co-creative approach characterizing the IMPULSE project.

Table 5: Requirements and values deriving from co-creation workshops

Value	Requirement
Technical robustness	The system should provide citizens with a solution that will be going for years, and the citizens do not need to change the practice. The system should provide citizens with a solution that will be going for years, and the citizens do not need to change the practice. The system should provide public administration a long-lasting solution so that public administration can avoid costly projects to upgrade new innovative solutions. The system should let citizens/entrepreneurs share/send data which are relevant for a specific purpose.
Usability and user friendliness	The system should provide public administration a better authentication process so that citizens identity information is easy to access for the administration. The system should provide dual identity for a citizen who wants to login for his own company and as a citizen so that login does not require multiple devices and credentials. The system should provide access to all the available digital services so that citizens do not have to manage diverse ways to access public services (1 app and 1 experience). The system should provide an authentication process through which a citizen can access a set of multiple public services and retrieve different information. The system should provide the access to a public service by registering only once so that it takes less time and is less prone to errors.

[31] For an overview of this approach see Cenci, A., Cawthorne, D. Refining Value Sensitive Design: A (Capability-Based) Procedural Ethics Approach to Technological Design for Well-Being. Sci Eng Ethics 26, 2629–2662 (2020). https://doi.org/10.1007/s11948-020-00223-3

Accessibility and inclusion by design	The system should let citizens to onboard identity without physically visiting a premise so that the authentication can be done when needed and not only during opening hours for the services The system should help to identify citizens using digital signature so that it can save costs of acquiring a digital signature. The system should support special issues of citizens such as a victim of an accident should be able to continue to use the account even if the person is disfigured in a way that affects recognition process. The system should provide a transgender person with an identification experience so that if my facial profile changes that does not affect for authentication. The system should provide elderly citizens a solution that is intuitive to use so that elderly citizens do not need extra training on how to use it.
Compliance to legal regulations, technical, and ethical standards	The system should have informed consent not only to be a document in legal language, but to be made interactive so that it is accessible also with dedicated icons. The system should notify the citizens any changes of the data so that citizens know how the data will be used or stored. The system should allow citizens to access the data so that they have control over who uses it and for what purpose. The system should provide European citizens a better way to align with the other national ID providers.
Security	The system should help a citizen to deactivate personal identity in case of mobile loss so that nobody can access services with that digital identity. The system should be able to ensure a breach of citizens credentials with a backup plan to adjust the situation. The system should have a good protection so that hackers cannot crack the system and do nefarious things. The system should provide notifications from the public administrations directly in the app so that the identity is trusted and valid.

5 Ethical and legal risks

No technology fits neutrally into the world, but all are used by different groups of users, for different purposes, and can have a more or less significant impact depending on the type of group they are adopted by. A society that would be led by decisions of policymakers to introduce some technological innovations that aim to revolutionise the way some established elements are conceived, risks making those technologies too disruptive for some fragile segments of the population (Dijik & Hacker, 2003)[32].

When it comes to an ethical assessment of digital identity, we need to introduce a preliminary clarification on what risks a paradigm of digital identity could lead to.

This the third step of the IMPULSE assessment method (section 2), which aim is to derive the **ethical** and **legal risks** that are associated with the Areas of Impact that are identified in the first step (section 4).

Performing an analysis from the deontological point of view has allowed the detection of the risks that are more general, while adopting the techniques of the value sensitive design other constraints and connected risks emerged, reflecting stakeholders concerns and values.

Therefore, detecting the risks associated with each value is a very important step into the IMPULSE assessment method because it allows to determine if and how the IMPULSE solution to eID manages to address and mitigate each risk.

After analysing the risks in the next subsections, section 6 will thus use them to assess the IMPULSE solution.

5.1 Identity management risks from a deontological perspective

By applying the deontological approach, subsection 4.1.14.1 has depicted a set of values and corresponding ethics principles on the identity and specifically on the Self Sovereign concept, adopted by the IMPULSE technological solution. Subsection 4.1.2 instead associates most of those values and principles to the GDPR articles. The following table defines potential risks with respect to the above values-principles-GDPR articles.

Table 6: Identity management risks from a deontological perspective

Value	Principle	GDPR Art.	Risk
			User-related
Wholeness	Existence	1, 3	Lack of an independent existence of users, making public and accessible too many aspects of their identity.
	Persistence	-	Identities are not long-lived, even in case some information on users changes
	Protection	25.1	Lack of protection of user identity
			Data-related
Autonomy	Control	24, 28, 12-22	Lack of control of their identities by users, who should be able to refer to them, update them, or even hide them at any time
	Access	15	Lack of access rights to their own data by users
	Minimisation	5	Disclosure doesn't involve the minimum amount of data necessary to accomplish the task at hand
	Consent	7	Lack of consent to the use of users' identity
			Architecture-related
Shareability	Transparency	5	Lack of transparency of IMPULSE technology and algorithms

[32] van Dijk, J. A. G. M., & Hacker, K. (2003). The digital divide as a complex and dynamic phenomenon. Information society, 19(4), 315-326. https://doi.org/10.1080/01972240309487

	Portability	**20**	Lack of portability of identity data
	Interoperability	**-**	Lack of availability of identities

5.2 Identity management risks from a value sensitive design perspective

As stated in subsection 4.2, through the value sensitive design approach, a set of general values and assumptions on the design of the technologies has been defined along with specific values expressed by the stakeholders through their requirements during the co-creation workshops. Those values are here associated to potential risks for the IMPULSE technological solution design and piloting.

Table 7: Identity management risks from a value sensitive design perspective

Value	**Risk**
	General Values
Feedback loop mechanism	Lack of stakeholder engagement during the IMPULSE technological solution design and implementation lifetime.
Freedom	Lack of information on the implementation process.
Guidelines	Lack of guidelines on how to embed ethics into the IMPULSE technological solution.
Disclosure	Lack of factual information regarding the stakeholders' involvement in the implementation process.
Consent	Lack of consent by the stakeholders during the implementation process.
Agreement	Lack of stakeholder freedom to leave the engagement at any point.
	Values identified during co-creation workshops
Technical robustness	The system is not technically designed in such a way that it can satisfy the needs of the citizens and of the public administration and is soon outdated, resulting in a waste of time and money for all the involved actors.
Usability and user friendliness	The system is not designed taking into account the stakeholders' needs (both citizens and the PA) and the resulting requirements and it is not sufficiently usable, so that in the end it is not adopted. In particular the problem of the siloed services and areas is a great risk because, if not solved, it would result in a disavowal of the users' requirements.
Accessibility and inclusion by design	The IMPULSE eID system is based on technologies like biometric identification and the blockchain (that lies at the basis of the implementation of the self-sovereign identity model) that could determine, because of biases and/or of bad design, a worsening of discriminatory outcomes with respect to certain categories (people going through gender transition, minorities, etc); furthermore, being a system heavily based on a digital access to services, it may increase the consequences of the digital divide on people who are already affected by it (for instance elderly or low alphabetized or poor people).
Compliance to legal regulations, technical, and ethical standards	Albeit the good intentions with respect to privacy and consent, the system might not be designed in such a way as to make it effectively easier for the citizen to understand and manage what consents he is giving and to whom, as well as to control how his personal data will be used or stored and for what purpose.
Security	According to a 2020 survey from the Eurobarometer[33] only 59% of people feel that they are able to protect themselves from ID theft and fraud[34]. One of the major worries with respect to digital identity is the possibility of identity theft or loss

[33] Available at https://europa.eu/eurobarometer/surveys/detail/2249
[34] https://europa.eu/eurobarometer/surveys/detail/2249

	and of malevolent data breach actions. The risk is that the cybersecurity plan is not sufficient as to guarantee an adequate level of security to all the stakeholders.

6 IMPULSE assessment

IMPULSE technological solution aims to be a novel electronic identity management (eID) system to be integrated into the online public services as a new and alternative eID option. Its architecture is built on a blockchain-based distributed Self-Sovereign identity model and a decentralized Identity paradigm.

As detailed in *D5.1 IMPULSE technology block - V1*, **the main architectural blocks of the IMPULSE solution that contribute to the realisation of the IDM and the Self-Sovereign identity model** are the following:

a) **The Blockchain-based infrastructure and SSI model** based on the European Blockchain Services Infrastructure and the European Self-Sovereign Identity Framework. EBSI vision is to leverage blockchain for the creation of cross-border services for public administrations and their ecosystems to verify information and make services trustworthy**.** Since 2020, EBSI is deploying a network of distributed blockchain nodes across Europe, supporting applications focused on selected use-cases. EBSI is the first EU-wide blockchain infrastructure, driven by the public sector, in full respect of European values and regulations. EBSI allows public administrations to protect against fraud, increase trust and security and make the verification of data authenticity easy and cost-efficient. It allows businesses to effortlessly interact with government agencies and reduce friction and administrative / compliance costs.

b) **The User Wallet** installed in the user device safeguards the user keys and personal information in an encrypted manner. In order to grant the user remaining with the full control of their personal data, that data can only be obtained when the user is verified by the different biometric methods involved during the digital onboarding process. The user wallet is able to communicate with the enterprise wallet, acting as the issuer and verifier of the credentials.

c) **The Smart Contract-based informed consent**, giving to the service users the opportunity of making their decisions about their data – such as who will have the permission of process their data, for which purpose, for how much time – using an easy-to-understand visual language based on graphical icons.

In addition, a specific subsection (6.3) will be dedicated to the use of **biometric data, in particular through facial recognition technique**. In fact, despite this technique does not pertain strictly to the definition of identity and to the related ethical, philosophical and legal questions, it brings a strong burden of discussion and disquiet, because of the possible implications that its adoption may generate.

6.1 Identity management contingency plan from a deontological perspective

The next table makes the assessment of the IMPULSE technological solution implementation for the IDM (i.e., the blockchain, the User Wallet and the Smart Contracts) in the light of the deontological perspective illustrated in section. Following the deontological approach, the assessment method is based on detecting the ethically and legally mandatory basing values, transforming them in risks and then evaluating whether the IMPULSE eID solution represents a valid answer to them. Thus, with the aim of showing how IMPULSE successfully copes with the main ethical and legal challenges, the following table contains the risks organised as for section 0, to which IMPULSE contingency plans are associated as well as the respective IMPULSE architectural blocks ensuring the success of the specific contingency plan.

Table 8: Contingency plans from a deontological perspective

Value	Principle	GDPR Art.	Risk	IMPULSE contingency plan	IMPULSE architectural block
			User-related		
Wholeness	**Existence**	**1, 3**	Lack of an independent existence of users, making	Natural persons are by virtue of this protected by the GDPR merely by reason of their existence, preferably with the	User Wallet

			public and accessible too many aspects of their identity.	encryption of their personal data. Through the minimisation principle, the protection mechanisms of users identity, as well as the provision of the User Wallet, IMPULSE paves the way for the independent existence of users.	
	Persistence	-	Identities are not long-lived, even in case some information on users changes	IMPULSE Blockchain is tamper-resistant and cannot be modified without a general consensus of the nodes. Therefore, unwanted or illegal modification of the chain, and therefore of the identities, is highly unlikely.	IMPULSE Blockchain
	Protection	**25.1**	Lack of protection of users identity	The decentralised public key infrastructure (DPKI) grants a cryptographic mechanism that by design allows for encryption of data and protection of the User (Sharma, 2019). IMPULSE provides the use of a distributed ledger with public/private keys, DIDs, credentials, as well as a network of multiple PAS, RAs, and encrypted communications strengthen data protection towards user's data self-sovereignty.	IMPULSE Blockchain
Autonomy			**Data-related**		
	Control	**24, 28, 12-22**	Lack of control of their identities by users, who should be able to refer to them, update them, or even hide them at any time	IMPULSE Sovereign Identity model is based on the Decentralized Identity paradigm: users have their single identity in their own IMPULSE User Wallet that they can manage autonomously.	User Wallet
	Access	**15**	Lack of access rights to their own data by users	IMPULSE smart contracts allow users to manage their consent, accessing it, revoking it at any time,	IMPULSE Smart Contracts

				visualising which entity is processing their identity. By using the graphical icons for consent management, users can easily make a complete decision about their data, such as who will have the permission of process their data, for which purpose, for how much time.	
	Minimalization	**5**	Disclosure doesn't involve the minimum amount of data necessary to accomplish the task at hand	Each digital identity will have a series of personal data strictly related to the service purpose, contained in the IMPULSE User Wallet.	User Wallet
	Consent	**7**	Lack of consent to the use of users identity	IMPULSE smart contracts implement all the required set of features for a complete informed consent management. In addition, a set of icons are integrated inside the IMPULSE application. The objective is to enable the representation of informed consents in a simplified way, simplifying understandability to final users.	IMPULSE Smart Contracts
			Architecture-related		
Shareability	**Transparency**	**5**	Lack of transparency of IMPULSE technology and algorithms	The chain of the IMPULSE blockchain where data are stored, given a public chain, is transparent to every node of the IMPULSE blockchain (and even to every user) and therefore fully auditable. This property increases reliability of B-Based IdM systems and also increases users' trust. Moreover, the icons used for users consent management provide a visual-based language with which users can make a	IMPULSE Blockchain, IMPULSE Smart Contracts

				complete decision about their data in a fully informed way, solving the long-lasting problem of understanding often hard to grasp consent forms. Thus, those icons try to reshape the consent-giving procedure, allowing for a more open and transparent mechanism in which, thanks to easily readable and accessible information provided by those visual cues, users have the opportunity to make significant decisions about their data.	
	Portability	**20**	Lack of portability of identity data	IMPULSE adopts the European Blockchain Services Infrastructure (EBSI) as the infrastructure for its own nodes. The EBSI Platform is a peer-to-peer network of interconnected nodes, operated at a national level by Member States' authorities mandated by the European Blockchain Partnership Policy group. EBSI allows citizens to take control of their data, secure them and easily move with their own credentials across Europe.	IMPULSE Blockchain
	Interoperability	**-**	Lack of availability of identities	The data stored in the chain of the IMPULSE Blockchain are highly interoperable between multiple different services and Relying Parties (entities devoted to the credentials verification).	IMPULSE Blockchain

6.2 Identity management contingency plan from a sensitive design perspective

The following table illustrates the IMPULSE proactive response to the design risks highlighted in section 5.2 related to the IMPULSE technological solution for the IDM, with reference to the blockchain, the User Wallet and the Smart Contracts. As mentioned in the preceding sections, using the deontological model a set of general mandatory ethical and legal values have been detected and defined. In this subsection, the identified values will act as the value basis of the value sensitive analysis, where both general issues taken from the literature and stakeholders views emerged during the WP2 co-creative workshops have been taken into consideration. The IMPULSE way of coping with them is then assessed through the identification of specific contingency plans. The aim is to made evident how IMPULSE manages to embed into the design of its solution the ethical

and legal values that are widely (generally in the EU and by the stakeholders) considered to be fundamental for any eID solution.

Table 9: Contingency plans from a user sensitive design point of view

Value	Risk	IMPULSE contingency plan
	General values	
Feedback loop mechanism	Lack of stakeholder engagement during the IMPULSE technological solution design and implementation lifetime	WP2 has been dedicated to the Co-creative design and piloting, stakeholders views have been translated into requirements
Freedom	Lack of information on the implementation process	• Delivering blueprint for enhanced eID public governance and public engagement • Delivering policy briefs for policy makers Incrementally gathering results thanks to the public engagement involving DIHs through the Digital Innovation Board
Guidelines	Lack of guidelines on how to embed ethics into the IMPULSE technological solution	Ethical and legal support through the definition of: • The IMPULSE ethical framework relevant for the research process (D1.2 Ethics protocol) • The legal framework relevant for the IMPULSE technology (D3.1 EU relevant legal framework) • the interdisciplinary vocabulary (D3.2 Ethical and legal dictionary) The evaluation of ethical issues raising from the analysis of technologies (D3.3 IMPULSE method for ethical and legal assessment)
Disclosure	Lack of factual information regarding the stakeholders' involvement in the implementation process	Provision of the information sheets for the pilot participants
Consent	Lack of consent by the stakeholders during the implementation process	Provision of the consent forms for the pilot participants
Agreement	Lack of stakeholders' freedom to leave the engagement at any point	Granting of the right to withdraw from the project involvement, with any consequence at any time
	Values identified during co-creation workshop	
Value	Risk	IMPULSE contingency plan
Technical robustness	The system is not technically designed in such a way that it can satisfy the needs of the citizens and of the public administration and is soon outdated, resulting in a waste of time and money for all the involved actors	The stakeholders have been consulted during the design phase embedding their needs into the requirements. A policy round table has also been held to take into account the policy makers views. Particular attention has been dedicated to the interoperability between IMPULSE and existing systems, which should grant both durability and scalability.
Usability and user friendliness	The system is not designed taking into account the stakeholders needs (both citizens and the PA) and the resulting	Two rounds of piloting activities have been foreseen, so as to collect users' feedback after the first round and, if necessary, to correct the user's

	requirements and it is not sufficiently usable, so that in the end it is not adopted. In particular the problem of the siloed services and areas is a great risk because, if not solved, it would result in a disavowal of the users' requirements.	interface before the second round. Great attention has been paid in the design phase to the easiness of use, using technologies such as biometric recognition and smart contracts, so as to make it the login to services process as smooth as possible.
Accessibility and inclusion by design	The IMPULSE eID system is based on technologies like biometric identification and the blockchain (that lies at the basis of the implementation of the Self-Sovereign Identity model) that could determine, because of biases and/or of bad design, a worsening of discriminatory outcomes with respect to certain categories (people going through gender transition, minorities, etc); furthermore, being a system heavily based on a digital access to services, it may increase the consequences of the digital divide on people who are already affected by it (for instance elderly or low alphabetized or poor people)	The issue that biometric identification could lead to biases and hidden discrimination has already been pinpointed in the D8.5 deliverable, where mitigation actions have been suggested. The issue of digital divide is a strong one that is common to all the projects that aim towards a stronger digitization of services, notably public services. It cannot be solved at the project level (its roots lie at the structural level of a country: its infrastructure, its instruction system, the wealth of its population) but at the national and European politics level, pointing to the necessity of policy actions to overcome it. One of the axes of the Next Generation EU plan is to promote the digitization of participating countries, through fundings and dedicated actions. In fact, all the countries part of the IMPULSE consortium are actively engaging to overcome the digital divide, which in some countries like Denmark pertains only the rural areas while in others, like Italy and Spain, is more diffused, also due to a high percentage of older population.
Compliance to legal regulations, technical, and ethical standards	Albeit the good intentions with respect to privacy and consent the system could not be designed in such a way as to make it effectively easier for the citizen to understand what consents he is giving and to whom and to manage them, as well as to control how his personal data will be used or stored and for what purpose	The use of the smart contracts, together with the development of dedicated icons to make always and immediately clear to the user the consents he is giving safeguards the IMPULSE eID system from this risk.
Security	According to a 2020 survey from the Eurobarometer only 59% of people feel that they are able to protect themselves from ID theft and fraud35. One of the major worries with respect to digital identity is the possibility of identity theft or loss and of malevolent data breach actions. The risk is that the cybersecurity plan is not sufficient as to guarantee an adequate level of security to all the stakeholders.	The IMPULSE approach to eID management relies on the blockchain and adopts a self-sovereign identity approach. These two-factors combined make almost impossible to steal one's personal data or identity.

From the results illustrated in the above tables it is quite clear that the IMPULSE approach to identity management, in particular for what pertains to its technological translation and implementation, is capable of effectively mitigating the risks and the issues emerging from the ethical and legal values that lie at its basis. In

[35] https://europa.eu/eurobarometer/surveys/detail/2249

other words, the IMPULSE project as it is implemented respects the explicit and the implicit ethical and legal requirements set up in the course of the project.

6.3 AI-based biometric facial recognition service

The IMPULSE project relies for the onboarding and for the subsequent identification of people on a form of AI-based biometric facial recognition. As it is widely known (and also analysed and assessed in the deliverable D8.5), **this technology may generate a number of unwanted consequences, the first one being that of the hidden biases**. Hereafter we examinate its general characteristics and how it is used inside IMPULSE, and we propose some contingency actions to potential risks it might pose. The assessment of this technique will continue during the next stages of the project, with the support of the policy makers that will be involved in future policy briefs organised by the project. Combined results will be reported in *D3.7 Recommendations on standards, ethical, legal and privacy issues*.

Facial recognition, paired with iris scan, handprint and fingerprint recognition, are the most promising biometric identification mechanism in which users can prove their identity. The GDPR (art 4.) defines biometric data as *"personal data resulting from specific technical processing relating to the physical, physiological 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"*. In the context of Impulse, a Facial recognition algorithm will be used in the process of **onboarding** (as per D5.1). Being easy to use and, being a biological feature of the individual, portable, difficult to lose and almost univocally capable of identifying someone, it could be considered a valuable mechanism to provide the first phase of onboarding and recognition of the Self-Sovereign Identity. However, as illustrated in the following subsections, from an ethical perspective, they pose a significant challenge when it comes to balancing the benefits and risks, and needs to be carefully evaluated[36][37].

6.3.1 Benefits

Table 10: Facial recognition benefits

Ease of use	Compared to other identification mechanism (such as the usual username and password) it is intuitively easier to use. It is estimated that on average a person have 100 passwords (Goodell & Aste, 2019)[38] and this biometric way of identification can ease the process of accessing digital services.
Precision	More stable than methods based on behavioural patterns (keystroke, voice print). The reason is that physiological features are often non-alterable. The behavioural patterns, on the other hand, may fluctuate due to stress, fatigue, or illness. Face recognition is one of the rare biometric technologies that combines high accuracy with little intrusiveness. It offers the precision of a physiological approach while being less obtrusive. As a result, face recognition has piqued the interest of academics in domains ranging from security, psychology, and image processing to computer vision. (Lin, 2000)[39]

[36] For a thorough analysis of the ethical issues raised by the use of biometric technologies as onboarding and identification systems inside digital identity systems see: Laas-Mikko, K., Kalvet, T., Derevski, R., Tiits, M. (2022). Promises, Social, and Ethical Challenges with Biometrics in Remote Identity Onboarding. In: Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., Busch, C. (eds) Handbook of Digital Face Manipulation and Detection. Advances in Computer Vision and Pattern Recognition. Springer, Cham. https://doi.org/10.1007/978-3-030-87664-7_20

[37] Christiane WENDEHORST, University of Vienna, Austria and Yannic DULLER, University of Vienna, Austria (2021) - Biometric Recognition and Behavioural Detection - Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 696.968 - August 2021 - ISBN 978-92-846-8436-6 doi: 10.2861/982599QA-02-21-976-EN-N. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

[38] Goodell, Geoffrey and Aste, Tomaso, A Decentralised Digital Identity Architecture (February 23, 2019). Frontiers in Blockchain, doi:10.3389/fbloc.2019.00017, Available at SSRN: https://ssrn.com/abstract=3342238 or http://dx.doi.org/10.2139/ssrn.3342238

[39] Shang-Hung, Lin. (2000). An Introduction to Face Recognition Technology. Informing Science The International Journal of an Emerging Transdiscipline. 3. 10.28945/569.

Uniqueness	Facial traits are unique in people, and a sound and consistent facial recognition algorithms allows for univocal identification of individuals (Balazia et al., 2020)[40]

6.3.2 Risks and Contingency plans

Table 11: Facial recognition risks and contingency plans

Risk	Description	IMPULSE contingency Plan
Security and Misuse	Facial recognition can be easily spoofed with various attacking methods such as photos, videos[41], or 3d masks (Erdogmus & Marcel, 2013) [42]	There exist known and tested anti spoofing methodologies like liveliness or eyeblink detection, or flash technology, that can detect if the system is being presented with a false face. Within IMPULSE the most advanced techniques have been adopted to support the onboarding and login system with ways of avoiding fraud.
Privacy	There is a problem of possible misuse: it has been showed that facial recognition mechanism can be bypassed by identifying strangers online (on a dating site where individuals protect their identities by using pseudonyms) and offline (in a public space), based on photos made publicly available on a social network site (Acquisti et al., 2015)[43]. On top of that, biometric data are considered by the GDPR with particular care, because it can enable the unique identification of an individual. The EU has already put strict rules in place under the Charter of Fundamental Rights, the General Data Protection Regulation, the Law Enforcement Directive and the EU framework on non-discrimination. (Madiega & Mildebrath, 2021)[44]	Within IMPULSE, the biometric data are not shared online or with an external identity provider but they are stored on the user's device. Therefore, unless the device itself is cracked, biometric data cannot be accessed other than by the owner of those data.
Technical Obstacles	There might be certain technical constraints of facial recognition algorithms that dampen the precision of the identification (Kaur et al., 2020)[45]: • Variable lighting conditions • Different poses • Facial occlusion • Facial expressions	This is a known problem. IMPULSE manages it by training the algorithm on real documents and faces in different light conditions or in different poses and conditions. One issue may be represented by the dimension of the campion, that in some countries is not sufficient. The IMPULSE

[40] Michal Balazia, S L Happy, Francois F Bremond, Antitza Dantcheva. How Unique Is a Face: An Investigative Study. ICPR 2020 - 25th International Conference on Pattern Recognition, Jan 2021, Milan / Virtual, Italy.

[41] https://towardsdatascience.com/facial-recognition-types-of-attacks-and-anti-spoofing-techniques-9d732080f91e, accesso il 24/03/2022

[42] Erdogmus, Nesli & Marcel, Sébastien. (2013). Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013. 1-6. 10.1109/BTAS.2013.6712688.

[43] Acquisti, Alessandro & Brandimarte, Laura & Loewenstein, George. (2015). Privacy and human behavior in the age of information. Science (New York, N.Y.). 347. 509-14. 10.1126/science.aaa1465.

[44] MADIEGA, T. & MILDEBRATH, H., 2021. Regulating facial recognition in the EU, EPRS: European Parliamentary Research Service.

[45] Kaur P, Krishan K, Sharma SK, Kanchan T. Facial-recognition algorithms: A literature review. Medicine, Science and the Law. 2020;60(2):131-139. doi:10.1177/0025802419893168

	• Age progression	consortium is working actively on this to deliver an absolutely accurate system.
Awareness	Data subjects' knowledge of facial recognition technologies and their influence on basic rights, as well as the general public's comprehension of them, should be actively promoted through accessible and instructive initiatives. "*The goal is to provide data subjects with simple concepts that can alert them before they decide to use facial recognition technology, to help them understand what it means to use sensitive data like biometric data, how facial recognition works, and to warn them about potential dangers, particularly in the event of misuse*". (Council of Europe, 2020)	The need for strong and dedicated communication actions emerged during the first policy round table and was incorporated as recommendation in the first policy brief. In the next months the Consortium will decide how to answer to the needs and ideas expressed in this respect by the policy makers.
Transparency	Like a Black Box Structure, the technology may exhibit a degree of opaqueness in which is not possible for the layman (and sometime for the technical practitioner) to understand its processes (Introna, 2005)[46]	Within IMPULSE, the issue arises only in the case of missed recognition, which in turn may cause delays or impossibility to access a service. In that case, human in the loop mechanisms are envisaged that can amend the wrong doing by the system. Researchers can of course use these cases to ameliorate the system. Since no decisions are taken by the algorithm and no complex reasoning is done by the system, the opacity can only be present in the lack of understanding of the reason why the access to service is denied. However, this is ascribable more to a technical defect (see "technical obstacles" for this) than to a black box mechanism.
Irrevocability	Biometric data cannot be modified or deleted: once an identity based on biometric data is created, it is not subject to change or deletion (as an account based on user name and password) and this in turn may cause a violation of the subject's rights	Within IMPULSE the biometric data are not accessible by third parties as they are stored in the data subject's device. In this way, even though they are immutable, the subject has full control whether to share them or not.
Dataization of the subject	When unique features of the subject (and in particular of the subject's body) are scanned and transformed into data, it is arguable that this in fact amounts to a true transformation of a subject's unique features and characteristics into data, that can then be exploited. This would be ethically questionable for various reasons, the first one being that it diminishes the dignity of the human person.	This may be true of centralized or federated identity management systems, where biometric data if used may be subject to unwanted exploitation. IMPULSE on the contrary adopts an SSI approach and the biometric data remain in control of the user and are used only for the onboarding and the authentication of the subject, remaining in its full control.
Violation of the human body	Biometric data are such a personal thing, pertaining to the physical characteristics of the subject (his/her body) that using them (a biometric template one created can be	Within IMPULSE only the facial recognition is used and only to allow to authenticate the subject for the first time. Then the biometric profile is deleted and the

[46] Introna, L.D. Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems. Ethics Inf Technol 7, 75–86 (2005). https://doi.org/10.1007/s10676-005-4583-2

	examined and scanned infinite ways by infinite subjects) could be assimilated to a violation of the human body, something that is not ethically acceptable	only operation that is performed is the matching between a selfie taken by the subject and a picture stored into his/her device. In this sense, the usage of the biometric data is very limited and no biometric template is created and shared.

7 Conclusions

With the aim of assessing the IMPULSE identity approach and the implemented technical solution from the ethical, legal and social perspective, the document defined a top-down methodology with the benefit of highlighting the strict relationship between ethics and technology, that in innovative projects such as IMPULSE cannot be underestimated.

First, following the deontological approach, the methodology has identified the set of foundational values and aims that in the IMPULSE relevant political and social area have to be respected. Then, ethical and legal risks have been derived from them and the design choices and implementation have been evaluated adopting a value sensitive design perspective, including the co-creative approach.

Following the user sensitive design approach, ethical values and risks have been transformed into technical ones and the way they have been mitigated through the IMPULSE technological solution implementation have been assessed with the following **general conclusions**:

- **The adopted methodology and the EU legal framework recognise that identity is more than an "administrative" identity** (name, age, place of birth, residence). In fact, it brings with it complexities and a constellation of many and different "attributes", varying over time but preserving the uniqueness and the persistence of the "digital" self. Attributes that the user, the sole detainer of his/her data, has the right to fully control.
- Thanks to its co-creative bottom-up approach adopted from the very first beginning of the project (the requirements identification phase), **the IMPULSE technological solution has taken into account the stakeholders' needs and opinions by design**.
- **IMPULSE lies perfectly in the context of EUDI Wallet pilots and experimentations**, respecting the values laid out by the European Commission and the more general values characterizing the EU and its current approach to identity management, especially with regard to the digital identity.

Therefore, the IMPULSE chosen approach, namely a decentralized, blockchain based SSI identity system, seems to have all the appropriate characteristics that should lie at the basis of an identity management system **fully respectful of the basic people's right** (as recognised and established inside the EU).

In particular, as it results from the assessment here performed, the IMPULSE eID solution has the following **ethically desirable characteristics**:

- It is respectful of people's rights to privacy and to control over their personal data and of the principle of data minimisation (GDPR).
- It is a system that grants the user freedom as to what do and to whom disclose access to his/her personal data. Since it is not centralized, the user is also free to withdraw from the system without risks of his/her identity continuing to be stored and accessed (Autonomy, Self Determination).
- It is secure, minimizing the risks of identity theft and spoofing (Security and Trust).
- It recognises that the identity of the person is not (only) a matter of administrative identification, that it includes numerous and complex attributes that may vary over time while the identity persists and that identity is more than the sum of basic demographic and biometric data (Existence, Persistence and Anti Reductionism).
- It is inclusive, helping also people with disabilities or impairments or living in rural areas to access public services (Equality and Inclusivity).
- It is transparent, as the blockchain nodes are fully inspectable and by means of specifically designed icons it makes fully understandable by the user what he/she is doing and the consents he/she is giving (Transparency).

- It is interoperable with other eID management systems, granting to the users a system that fully works (Interoperability).
- It is reachable even when the user has not with him his/her physical id card or his/her account, as it relies only on biometric authentication for the log in, being in this way accessible from anywhere (Usability, Portability).
- Making identity persistent through the different services, it also promotes a stronger responsibility and accountability of the subject (Moral responsibility of the subject).
- Through its co-creative approach, it is respectful of the stakeholders views and embeds them in the design of the technical solution (Usability, Value Sensitiveness).
- Finally, it enhances participation and engagement of citizens, making it easier for the people to contact and communicate with the public administration and to use services online (Engagement and Participation).

Finally, it results evident that the IMPULSE eID system **has the potentiality to be an acceptable technology that will significantly improve the quality of people's lives**.

However, there are some **potential concerns** that can be summarised as follow:

- Every identity management choice brings **complexities and ethical consequences often unrecognized** but that could have a great impact on people's lives and rights. Therefore, governments and policy makers should be very careful as to which digital identity management system to adopt.
- There are sectors of the population that may not be able to use IMPULSE (or any other similar eID system) due to the **existent digital divide**. Therefore, while this being an unavoidable side consequence of the digitisation, every effort should be put into minimising its impacts, by systematically bringing forward dedicated actions such as, for instance:
  - ⇒ a strong digitisation plan bringing fast-internet also in rural areas and widening the access to dedicated devices also to poor or disadvantaged people.
  - ⇒ ideate and perform targeted education and communication actions.
  - ⇒ design human-in-the-loop schemes and supporting actions when people for any reason do not manage to access public services through IMPULSE.

As per the next steps, **the assessment of relevant ethical, legal and social issues will continue during the project in combination with the formulation of the policy recommendations**. For instance, the use of biometric identification inside the IMPULSE eID solution, here discussed and assessed in section 6.3, might need a further analysis from the political standpoint, that will be provided by the deliverable *D3.7 Recommendations on standards, ethical, legal and privacy issues*.

References

[1] Acquisti, Alessandro & Brandimarte, Laura & Loewenstein, George. (2015). Privacy and human behavior in the age of information. Science (New York, N.Y.). 347. 509-14. 10.1126/science.aaa1465.

[2] Allen, C. The Path to Self-Sovereign Identity. 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereereign-identity.html

[3] Aims and Values of the European Union - https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en

[4] Michal Balazia, S L Happy, Francois F Bremond, Antitza Dantcheva. How Unique Is a Face: An Investigative Study. ICPR 2020 - 25th International Conference on Pattern Recognition, Jan 2021, Milan / Virtual, Italy.

[5] Mario De Caro and David Macarthur (eds) Naturalism in Question. Cambridge, Mass: Harvard University Press, 2004.

[6] Devon, R.E. and Ibo van de Poel. "Design Ethics: The Social Ethics Paradigm*." International Journal of Engineering Education 20 (2004): 461-469.

[7] Erdogmus, Nesli & Marcel, Sébastien. (2013). Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013. 1-6. 10.1109/BTAS.2013.6712688.

[8] Flathman, R. (2006). In the Beginning Was the Deed: Realism and Moralism in Political Argument. Perspectives on Politics, 4(2), 375-376. doi:10.1017/S1537592706320270

[9] Friedman, B., Kahn, P.H., Borning, A., Huldtgren, A. (2013). Value Sensitive Design and Information Systems. In: Doorn, N., Schuurbiers, D., van de Poel, I., Gorman, M. (eds) Early engagement and new technologies: Opening up the laboratory. Philosophy of Engineering and Technology, vol 16. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-7844-3_4

[10] Friedman, B., Kahn, P., & Borning, A. (2002). Value sensitive design: Theory and methods. University of Washington technical report, 2, 12.

[11] Friedman, B., Kahn, P.H., Borning, A., & Huldtgren, A. (2020). Value Sensitive Design and Information Systems. The Ethics of Information Technologies.

[12] Friedman, B., Millett, L., and Felten, E. (2000). Informed Consent Online: A Conceptual Model and Design Principles. University of Washington Computer Science & Engineering Technical Report 00–12–2

[13] Goodell, Geoffrey and Aste, Tomaso, A Decentralised Digital Identity Architecture (February 23, 2019). Frontiers in Blockchain, doi:10.3389/fbloc.2019.00017, Available at SSRN: https://ssrn.com/abstract=3342238 or http://dx.doi.org/10.2139/ssrn.3342238

[14] Hendry, D.G., Friedman, B. & Ballard, S. Value sensitive design as a formative framework. Ethics Inf Technol 23, 39–44 (2021). https://doi.org/10.1007/s10676-021-09579-x

[15] IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity - Available at: https://ec.europa.eu/newsroom/dae/redirection/document/76618

[16] Introna, L.D. Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems. Ethics Inf Technol 7, 75–86 (2005). https://doi.org/10.1007/s10676-005-4583-2

[17] Ishmaev Georgy, Stokkink Quinten, Identity Management Systems: Singular Identities and Multiple Moral Issues, Frontiers in Blockchain Vol 3 2020, https://www.frontiersin.org/articles/10.3389/fbloc.2020.00015

[18] Ishmaev G. Sovereignty, privacy, and ethics in blockchain-based identity management systems. Ethics Inf Technol. 2021;23(3):239-252. doi: 10.1007/s10676-020-09563-x. Epub 2020 Nov 30. PMID: 33281497; PMCID: PMC7701220.

[19] Kaur P, Krishan K, Sharma SK, Kanchan T. Facial-recognition algorithms: A literature review. Medicine, Science and the Law. 2020;60(2):131-139. doi:10.1177/0025802419893168

[20] Lessig, L. (2006). Code and Other Laws of Cyberspace, Version 2.0. New York: Basic Books.

[21] Loffreto, Devon. 2016. "Self-Sovereign Identity". The Moxy Tongue.https://www.moxytongue.com/2016/02/self-sovereign-identity.html

[22] Loffreto, Devon. 2012. "What is 'Sovereign Source Authority'?" The Moxy Tongue. http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

[23] MADIEGA, T. & MILDEBRATH, H., 2021. Regulating facial recognition in the EU, EPRS: European Parliamentary Research Service.

[24] Manders-Huits, N. (2010). Practical versus moral identities in identity management. Ethics Information Technol. 12, 43–55. doi: 10.1007/s10676-010-9216-8 DOI=10.3389/fbloc.2020.00015

[25] Shang-Hung, Lin. (2000). An Introduction to Face Recognition Technology. Informing Science The International Journal of an Emerging Transdiscipline. 3. 10.28945/569.

[26] Stallman, Richard: Free Software, Free Society: Selected Essays of Richard M. Stallman (Boston: GNU Press, 2002), ed. by Joshua Gay, contrib. by Lawrence Lessig

[27] Stilz, Anna, 'Introduction: The Normative Bases for Territorial Sovereignty', Territorial Sovereignty: A Philosophical Exploration, Oxford Political Theory (Oxford, 2019; online edn, Oxford Academic, 24 Oct. 2019), https://doi.org/10.1093/oso/9780198833536.003.0001

[28] van Dijk, J. A. G. M., & Hacker, K. (2003). The digital divide as a complex and dynamic phenomenon. Information society, 19(4), 315-326. https://doi.org/10.1080/01972240309487

[29] Wang, Fennie and De Filippi, Primavera, Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion (January 23, 2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, in Frontiers in Blockchain (Special Issue on Identity and Privacy Governance), 2020, Available at SSRN: https://ssrn.com/abstract=3524367

[30] Wang, Fennie and De Filippi, Primavera, Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion (January 23, 2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, in Frontiers in Blockchain (Special Issue on Identity and Privacy Governance), 2020, Available at SSRN: https://ssrn.com/abstract=3524367

[31] Zwitter, Andrej and Gstrein, Oskar Josef and Yap, Evan, Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual (March 4, 2020). Front. Blockchain, 28 May 2020 | https://doi.org/10.3389/fbloc.2020.00026, Available at SSRN: https://ssrn.com/abstract=3454513 or http://dx.doi.org/10.2139/ssrn.3454513

[32] Zwitter, Andrej and Gstrein, Oskar Josef, Editorial: Identity and Privacy Governance (August 06, 2021). Frontiers in Blockchain 2021, Available at SSRN: https://ssrn.com/abstract=3906511