EPICENTER .WORKS
for digital rights

The View from Brussels on the DPI Safeguards Debate:

Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures

29. February 2024 (v2)

EXECUTIVE SUMMARY

This report analyses the human safeguards developed for Digital Public Infrastructure (DPI) systems in EU law. We detail mechanisms that aim to foster trust and inclusion in these systems and provide for state of the art privacy-by-design. Nine key recommendations to mitigate concrete harm are exemplified in their effect and detailed with legal text:

1. Every citizen or resident of a country has a right to obtain digital identity free of charge. Use of the DPI is voluntary and horizontal obligations protect persons that are not using the system from being excluded, denied goods or services or disadvantaged in the private or public sector.
2. A user interacting on a DPI system always knows the identity of the other party before personal information is exchanged. Who is asking makes a difference. Any information category asked from a user must be in a public registry of all DPI use cases. Users can file complaints and companies can be excluded from the DPI ecosystem.
3. No personal information is shared without the users consent. A user can choose to comply with a request for information fully, not at all or partially by only selectively disclosing parts of the information they have been asked for.
4. A privacy-by-design architecture prevents the operating authority of the DPI to obtain information about concrete user behaviour, without that users consent. Daily interactions on the DPI are invisible for the government and connected companies.
5. A user interacting via the DPI with other parties is protected from tracking and profiling by privacy-enhancing technologies like pairwise-pseudonymous identifiers, zero-knoweldge proofs and unlinkability. A user cannot be identified with just one unique and persistent identifier.
6. Users have a right to use freely chosen Pseudonyms not linked to their real identity whenever there is no legal obligation that they have to identify themselves.
7. All DPI components must at be available open source for public scrutiny. Tax-payer funded DPI must be available under a free software licence.
8. A full list of transactions has to be available to the user of the DPI. This includes the identity of all parties the user interacted with, any information shared and means to request deletion.
9. Biometric authentication shall not be a precondition for using DPI. There must be a way to obtain a digital identity and use DPI without handing over biometrical information. Storage of

biometrical information on a central server requires prior explicit consent from the user. Biometrical information has to be specially protected.

Executive Summary 1
Introduction 2
Terminology and Sources 3
Recommendation 1: Accessible, cost-free and Voluntary 4
Recommendation 2: Use Case Regulation 5
Recommendation 3: Zero-Knowledge and Selective Disclosure 8
Recommendation 4: Unlinkability and Unobservability of User Behaviour 10
Recommendation 5: No Unique Persistent Identifiers 13
Recommendation 6: Right to Pseudonymity 15
Recommendation 7: Free and Open Source 16
Recommendation 8: Privacy Cockpit 17
Recommendation 9: No Requirement for Biometrics 18

INTRODUCTION

Epicenter.works is a digital rights NGO working on human-centered technology since 2010. We work on DPI since 2017. Our mission is to promote and defend human rights in the digital age and to work towards a positive, empowering effect of technology in society. Our methods include high level advocacy, in-depth research, strategic litigation and building participatory online campaigns. Key achievements include the abolishment of EU data retention surveillance laws, enshrining net neutrality in EU law or safeguards in DPI created during the COVID-19 pandemic[1].

The aim of this report is to critically analyse which lessons has EU law-making taught us that could contribute to the development of global standards for Digital Public Infrastructure (DPI). The result is an analysis of human rights safeguards for DPI systems developed in EU law during the legislative term 2019-2024 and a series of recommendations. Based on the experience from EU legislation, it aims to identify the lessons for concrete legal and technical human rights protection mechanisms in the context of DPI. A particular focus is given to privacy-by-design and inclusiveness.[2] The European legislator did not find the General Data Protection Regulation (GDPR) to already provide sufficient safeguards for DPI. Since the GDPR was approved in 2015 and came into effect in 2018 all safeguards outlined in this paper go beyond the GDPR and are specific to DPI systems.

Target audience of this paper are decision makers outside the EU, researchers, technicians and CSOs interested in DPI and specifically digital identity systems. The research question of this report is to identify the concrete safeguards for DPI system that were developed in European law. We hope to export good ideas into the ongoing UN process to agree on DPI safeguards globally[3]. Subsequently, we also want to open the debate about legislative safeguards for a technical audience, that is now tasked with implementation and standardization.

1 Full history: https://en.epicenter.works/history
2 In the EU debate the important issue of the right to legal identity (SDG 16.9) was not central and is therefore not covered here.
3 https://dpi-safeguards.org

This paper focuses mainly on the eIDAS reform that establishes a general purpose digital identification and attribute verification infrastructure and also includes examples of safeguards adopted in the COVID-19 emergency legislation for vaccination/recovery/testing certifications. Given the slow negotiations, we could not take into account the proposal for a possible digital euro to establish a Central Bank Digital Currency (CBDC)[4]. In our role as civil society watchdog, we followed these three dossiers closely and were in permanent contact with lawmakers regarding the adoption of proper safeguards in all three proposals[5]. This paper introduces safeguards in a generalized way and exemplifies them with concrete legal language.

Terminology and Sources

DPI Systems: While many stakeholders reference the changing definition of DPI[6], in this report we define it as digital systems, services and interfaces created by or on behalf of a public authority for the purpose of being used by citizens, residents and the private sector. The core of every DPI is a digital identity system for natural and/or legal persons. Often it includes platforms for payments and the exchange of (personal) information. In contrast the term Public Digital Infrastructure focuses more on such systems providing public-value alternatives to existing commercial platforms in areas like social media or proprietary software.[7] Importantly, DPI does not encapsulate telecommunications infrastructure.

eIDAS Regulation: The term "eIDAS Regulation" refers to an updated version of this law, which includes the 2021-2024 reform. Whenever the "eIDAS Regulation" is mentioned, we refer to the approved legal text[8]. The legislation was approved on 29 February 2024 by the European Parliament.[9] To better outline concrete implementations of certain safeguards we might also refer to earlier version of the legal text as it was adopted in the plenary or by the rapporteur in the European Parliament. The references to the legal text of those versions can be found in the footnotes.

The eIDAS Regulation establishes a cross-border, general purpose digital public infrastructure. This system is called the "European Digital Identity Wallet" (in short: EUDI Wallet or EDIW) and it allows natural or legal persons to identify themselves, verify attributes about them, authenticate them (logging into a service) or sign legally binding contracts vis-a-vis the private and public sector. Both the attributes within the system and the relying parties with whom a user interacts, can be any public or private entity as long as they follow the Regulation. The eIDAS Regulation establishes the legal framework, binding inter-operability specifications and certification mechanisms for the creation of national implementations of the EUDI Wallet that every Member State is obliged to offer to natural and legal persons in their territory.

Relying parties: The term "relying parties" refers to the company or public entity with which a user interacts when using the DPI.

EU Digital COVID Certificate Regulation: We also refer to the "EU Digital COVID Certificate Regulation", which was adopted in 2021. The legal text is published in the official journal of the EU.[10]

4 Our policy analysis of the Commission proposal:https://epicenter.works/content/right-to-cash-and-digital-euro-policy-analysis-from-a-human-rights-perspective
5 Repository of submissions available via the filters "eID", "COVID-19" or "digital Euro": https://en.epicenter.works/documents
6 https://www.undp.org/digital/digital-public-infrastructure
7 https://openfuture.eu/our-work/public-digital-infrastructure/
8 https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_EN.pdf
9 https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/0136(COD)
10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953

This emergency legislation established technical ways to prove a person's vaccination, recovery or testing status during the pandemic. The architecture followed a high privacy-by-design standard which makes it relevant to this debate.

We exemplify safeguards by providing legal text according to the following rules:

Boxes with double borders contain legal text that was approved by the European Union.

Boxes without a border contain text that was officially tabled in the negotiation process, but did not make it into the final text.

Legal provisions that fully implement the safeguard are demonstrated in a green box, whereas legal text that only partially fulfils the requirement are highlighted in yellow boxes. Finally, legal text outlined in red boxes undermines safeguards. A text below every box reiterates this for accessibility reasons. **Highlights** throughout the legal text are added by the authors to exemplify certain provisions.

RECOMMENDATION 1: ACCESSIBLE, COST-FREE AND VOLUNTARY

A key safeguard in the establishment of DPI systems is their voluntary and accessible nature. The eIDAS proposal was accompanied by such a political promise from the European Commission[11]. In fact, the voluntary nature was enshrined on three layers: First, every user with a citizenship or residency in a EU member state has a right to an EUDI Wallet in their own name. Secondly, the EUDI Wallet must be offered to all natural persons free of charge.

Thirdly, this Commission proposal was further strengthened by the European Parliament which introduced a protection against discrimination for everyone choosing not to use the EUDI Wallet in any particular situation that concerns access to government services, freedom to conduct business or the labour market. This means that any person deciding not to use the EUID Wallet must not suffer negative consequences for opting-out, like being refused a service, asked to pay a higher price for it or hindered in any way.

The goal of all these provisions is to ensure that the rights of individuals are protected, independently of their income, age, digital or legal literacy, legal residency or any other relevant status. Also, rights should be protected regardless of the technology someone is (not) using – like dependency of DPI on up-to-date smartphones from Google, Apple or third party vendors or the willingness to authenticate oneself with biometrics. Such safeguards have to take into account the fact that these DPI systems do not exist in isolation and solely relying on the users' consent would often re-enforce existing power imbalances in society. Therefore, eIDAS ensures that different pathways besides the DPI have to remain available and people not relying on the EUDI Wallet have to be provided fair and equal access.

Article 5a of the eIDAS Regulation:

> *"(1) For the purpose of ensuring that **all natural and legal persons in the Union** have secure, trusted and seamless cross-border access to public and private services, while having*

11 https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_2664

full control over their data, each Member State shall provide at least one European Digital Identity Wallet.
[...]
(13) The issuance, use and revocation of the European Digital Identity Wallets shall be ***free of charge to all natural persons.***
[...]
(15) ***The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.****"*

Fully DPI-safeguard compliant provision that was adopted.

RECOMMENDATION 2: USE CASE REGULATION

Any DPI systems that allow the private sector to obtain personal information brings unique challenges that have to be met with proportional safeguards. It is vital to stress that the EU lawmakers found that the General Data Protection Regulation (GDPR) of the EU does not provide sufficient safeguards for DPI. Among the many safeguards outlined for in this report, the regulation of use cases is a central one. Use-cases refer to any type of application of the DPI by a relying party in their processes. For example, when the DPI is used by a bank verify the identity of a potential account holder, by a car rental company checking someones driver licence or by a pharmacy receiving the prescription of a client.

A core premise of the legislator was the risk of *over-identification* and *over-sharing*, which means that in many situations user consent is not a sufficient protection against the overreaching transfer of personal information to third parties and the excessive identification in previously anonymously conducted interactions. The personal information in DPI is available in standardized form with the cryptographic signatures of the government that ensures its authenticity. In many situations the power-dynamics or necessity to obtain certain goods or services make the refusal of consent by the user unrealistic and would over-burden the user. Examples would be border crossings, requests for information in a hospital or late night hotel checkins. The success of the DPI also depends on the trust that citizens place in it, which is influenced by the ecosystem where its used. If bad actors are free to participate in the system and obtain authentic information without a proper legal basis, citizens would have to stop using the DPI to protect themselves.

The EU approach to use case regulation is a multi-layered framework that starts with the registration of all public and private relying parties with each of their use cases. This includes for each relying party their names, country of establishment, contact information, intended use case(s) and – importantly – the information they plan to request from users via the DPI for each of their use cases. Relying parties can only ask from users the information according to their registration. The full list of registered relying parties must be available online in machine-readable format:

Article 5b of the eIDAS Regulation:

> *"(1) Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the* ***relying party shall register in the Member State where it is established****.*
>
> *(2) The registration process shall be cost-effective and proportionate-to-risk. The* ***relying party shall provide at least:*** *(a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes: (i)* ***the Member State in which the relying party is established****; and (ii)* ***the name of the relying party*** *and, where applicable, its registration number as stated in an official record together with identification data of that official record; (b) the* ***contact details*** *of the relying party; (c)* ***the intended use of European Digital Identity Wallets, including a indication of the data to be requested by the relying party from users.***
>
> *(3)* ***Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).***
>
> *(4) Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.*
>
> *(5)* ***Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.***
>
> *(6) Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2. […]"*

Fully DPI-safeguard compliant provision that was adopted.

Before the user is asked to provide their personal information to a relying party, the latter has to provide them with their identification. The users decision to hand over information might depend on the trustworthiness of the one who asks. For all these steps, the relying party needs to have an active registration (see above). The identification of the relying party is assured at the same high level as the users identification. The DPI offers the user a functionality to report any suspicion of unlawful behaviour of the relying party to the national authority where the relying party is established, which can lead to their registration being revoked. Particularly sensitive information, like health data, can be protected with "disclosure policies" that further limit who is allowed to ask for that information.

Article 5b(8) of the eIDAS Regulation

> "*Where relying parties intend to rely upon European Digital Identity Wallets,* ***they shall identify themselves to the user****."*

Article 5a(5) of the eIDAS Regulation:

> *"European Digital Identity Wallets shall, in particular: (a) support common protocols and*

interfaces: [...]

*(vii) for authenticating and **identifying relying parties** by implementing authentication mechanisms in accordance with Article 5b; [...]*

*(x) for **reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received**;*

[...]

*(e) **in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation;**"*

Fully DPI-safeguard compliant provision that was adopted.

Should certain sectors be under a legal or contractual obligation to identify their users or customers, the EU obliges them to offer the DPI as a means to do so. Dominant internet companies[12] are also obliged to offer the DPI as a means of logging into their services. The user is always free to use the DPI and they need to be offered an alternative (see above safeguard "Accessible, cost-free and Voluntary"). This measure aims to proliferate the DPI by forcing large parts of the private sector to adopt it and offer it to their customers and visitors. A more appropriate way would have been to limit the use of DPI to cases where legal obligations require the relying party to identify the user and not include contractual obligations as a legitimate basis.[13] Particularly, the proliferation of the DPI in very data hungry sectors like social media and targeted advertisement increases the risk of profiling and is not proportional for a trust-based system.

Article 6db of the eIDAS Regulation:

*"(2) Where private relying parties that provide services, **with the exception of microenterprises and small enterprises** as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC, are **required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation**, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and **only upon the voluntary request of the user**, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.*

*(3) Where providers of **very large online platforms** as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council require user authentication for*

12 List of so called Very Large Online Platforms in Europe that fall under this obligation: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

13 https://epicenter.works/content/digital-identity-open-letter-on-eidas-reform-to-the-european-parliament and https://epicenter.works/content/eidas-policy-analysis-english

access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication ***only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested****."*

Non-DPI-safeguard compliant provision that was adopted.

Lastly, should intermediary services act on behalf of relying parties they must follow the same obligations and they are prohibited from storing data about the content of the transaction. An example would be point of sales terminals in which the age verification is done on behalf of a store owner. Such intermediaries might be concentration points that integrate the DPI in existing software and hardware solutions. Hence, they could be party to the transactions of many other companies or sectors. In the questions and answers between the Commission and the European Parliament it was clarified that such intermediaries could also be blind towards the content of the transactions by simply passing encrypted information along as proxies.

Article 5b (10) of the eIDAS Regulation:

*"****Intermediaries*** *acting on behalf of relying parties* ***shall be deemed to be relying parties*** *and* ***shall not store data about the content of the transaction****."*

Fully DPI-safeguard compliant provision that was adopted.

RECOMMENDATION 3: ZERO-KNOWLEDGE AND SELECTIVE DISCLOSURE

Zero-Knowledge checks provide a privacy-respecting way to verify if certain attributes or attribute combinations about a person are true. A simple example is to verify whether a person is of legal age without revealing their birthdate. This has become a standard for modern digital identity systems[14] and is a precondition for making DPI systems safe according to modern standards. Subsequently, when attributes are exchanged between a user and a relying party, the system should prevent linkability of the user across interactions with the same or different relying party in all cases where full identification of the user is not required. For example, someone verifies their age in a club every Friday and the owner doesn't know its the same person. Lastly, whenever a relying party requests information from a user, they need to be able to hand over everything, nothing or "selectively disclose" only parts of the information that has been requested from them. For example, a request for name and family status could be partially refused by only handing over one of these data points.

These technical requirements all benefit the protection against tracking and profiling of user behaviour. They are vital for putting users into control, to offer a functionality of the DPI that only makes that personal information available to the relying party for which an informed consent has been obtained. Even after information is shared, no later interactions of that user with the same or other relying parties should allow to infer behaviour or profile them.

14 ISO standard for the mobile driving license 18013-5

Article 5a(16) of the eIDAS Regulation:

> *"The technical framework of the European Digital Identity Wallet shall:*
> *(b) enable **privacy preserving techniques which ensure unlinkability**, where the attestation of attributes does not require the identification of the user.."*

Article 5a(4):

> *"European Digital Identity Wallets shall enable the user, in a manner that is **user-friendly, transparent, and traceable by the user**, to:*
>
> *(a) securely request, obtain, select, combine, store, delete, share and present, **under the sole control of the user**, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while **ensuring that selective disclosure of data is possible**;"*

Recital (59):

> *"**Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user**. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. It should be technically possible for the user to selectively disclose attributes, including from multiple, distinct electronic attestations, and to combine and present them seamlessly to relying parties. This feature should become a basic design feature of European Digital Identity Wallets, thereby reinforcing convenience and the protection of personal data, including data minimisation."*

Recital (14):

> *"Member States should integrate different privacy-preserving technologies, such as **zero knowledge proof**, into the European Digital Identity Wallet. Those cryptographic methods should allow a relying party to validate whether a given statement based on the person's identification data and attestation of attributes is true, without revealing any data on which that statement is based, thereby preserving the privacy of the user."*

Fully DPI-safeguard compliant provision that was adopted.

RECOMMENDATION 4: UNLINKABILITY AND UNOBSERVABILITY OF USER BEHAVIOUR

To be safeguards-compliant, the architecture of DPI has to follow the same fundamental rights principles as the design of analogue public systems. That entails that daily interactions of innocent people shouldn't be subject to government surveillance without probable cause. Such protection following the privacy-by-design principle must prevent, on a technological level, that user interactions can be observed by a third party, particularly the issuing or operating authority of the DPI (the government and their contractors). The term used for this concept in the European discussion is "*unobservability*".

Unobservability entails the concept of unlinkability for the individual inter-actions between a user and various relying parties, whereby the correlation of these interactions with each other is prevented.[15] But unobservability goes beyond that, as it also restricts what information the issuing or operating authority of the DPI is able to obtain.

Unobservability cannot be achieved by solely relying on administrative restrictions about what information can be accessed by whom under what circumstances. Moreover, the concrete technical architecture has to be designed in a way as to prevent such information to ever be obtained by the public body in charge of the DPI or organisations connected to it, without the informed consent of the affected user(s).

Such architectural protection of privacy is necessary since the ubiquitous nature of many DPI systems enables them to spread towards all areas of life (finance, health, commerce, justice, social media, etc.). Being able to combine behavioural information about all these areas of life on a population level would amount to a panoptical level of surveillance pressure which would violate the essence of the right to privacy.[16]

The concept of unobservability was first enshrined in the legislative term 2019-2024 in the regulation to establish EU Digital COVID Certificates.

Article 4(2) of the EU Digital COVID Certificate Regulation:

> *"The trust framework shall be based on a public key infrastructure and allow for the reliable and secure issuance and verification of the authenticity, validity and integrity of the certificates referred to in Article 3(1). The trust framework shall allow for the detection of fraud, in particular forgery. In addition, it may support the bilateral exchange of certificate revocation lists containing the unique certificate identifiers of revoked certificates. Such certificate revocation lists shall not contain any other personal data.* ***The verification of the certificates referred to in Article 3(1) and, where applicable, certificate revocation lists shall not give rise to the issuer being notified of the verification.***"

15 This is to be distinguished from the use case where a user wants to be recognized by a relying party, for example to access his previous orders or his bank account.

16 The global nature of DPI spanning across jurisdictions and the retention period of any behavioural data factor into the privacy footprint of these systems.

Recital 22 and 55 of the EU Digital COVID Certificate Regulation:

> *"(22) The security, authenticity, validity and integrity of the certificates making up the EU Digital COVID Certificate and their compliance with Union data protection law are key to their acceptance in all Member States. It is therefore necessary to establish a trust framework laying out the rules on and infrastructure for the reliable and secure issuance and verification of COVID-19 certificates. The infrastructure should be developed, with a strong preference for the use of open-source technology, to function on different major operating systems, while ensuring that it is protected from cybersecurity threats.* ***The trust framework should ensure that the verification of COVID-19 certificates can be carried out offline and without the issuer or any other third party being informed about the verification.*** *The trust framework should be based on a public-key infrastructure with a trust chain from Member States' health authorities or other trusted authorities to the individual entities issuing the COVID-19 certificates. The trust framework should allow for the detection of fraud, in particular forgery. The eHealth Network's Outline Interoperability of Health Certificates Trust Framework of 12 March 2021 adopted pursuant to Article 14 of Directive 2011/24/EU of the European Parliament and of the Council (8) should form the basis for the trust framework for the EU Digital COVID Certificate.*
>
> *(51) For the purposes of this Regulation, personal data on individual certificates do not need to be transmitted or exchanged across borders.* ***In line with the public-key infrastructure approach, only the public keys of the issuers need to be transferred or accessed across borders, which will be ensured by an interoperability gateway set up and maintained by the Commission.*** *In particular, the presence of the certificate combined with the public key of the issuer should allow for the verification of the authenticity, validity and integrity of the certificate.* ***To prevent and detect fraud, Member States should be able to exchange lists of revoked certificates. In line with the principle of data protection by default, verification techniques not requiring transmission of personal data on individual certificates should be employed.****"*

Fully DPI-safeguard compliant provision that was adopted.

Similar provisions can be found in the eIDAS Regulation. Their goal is to ensure that the providers of attributes or other connected companies to the system cannot obtain information about the concrete user behaviour. This provision achieves, for example that a university would not obtain information about one of their alumni showing the digital version of their diploma to a potential employer.

Article 5a of the eIDAS Regulation:

> *"(16)* ***The technical framework of the European Digital Identity Wallet shall****: (a)* ***not allow providers of electronic attestations of attributes or any other party****, after the issuance of the attestation of attributes,* ***to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user****;*
> *[...]*
>
> *(5) European Digital Identity Wallets* ***shall, in particular****: [...] (b)* ***not provide any information to trust service providers of electronic attestations of attributes about***

the use of those electronic attestations;"

Fully DPI-safeguard compliant provision that was adopted.

The issuing or operating entity of the DPI is also under an obligation not to obtain information about the user interactions, without their explicit consent or in cases where it is unavoidable for the provision of the service. This text was negotiated up until the last minute and lacks legal clarity.

Article 5a(7) of the eIDAS Regulation:

> "***Users shall have full control of the use of and of the data in their European Digital Identity Wallet***. *The* ***provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third- party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise.*** *Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply mutatis mutandis."*

Recital (32):

> *"The use, free of charge, of European Digital Identity Wallets should not result in the processing of data beyond data that is necessary for the provision of European Digital Identity Wallet services. This Regulation should not allow the processing of personal data stored in or resulting from the use of the European Digital Identity Wallet by the provider of the European Digital Identity Wallet for purposes other than the provision of European Digital Identity Wallet services.* ***To ensure privacy, European Digital Identity Wallet providers should ensure unobservability by not collecting data and not having insight into the transactions of the users of the European Digital Identity Wallet. Such unobservability means that the providers are not able to see the details of the transactions made by the user****. However, in specific cases, on the basis of* ***explicit prior consent by the user in each of those specific cases****, and fully in accordance with Regulation (EU) 2016/679, providers of European Digital Identity Wallets could be granted access to the information necessary for the provision of a particular service related to European Digital Identity Wallets."*

Partially DPI-safeguard compliant provision that was adopted.

A clearer formulation of that same principle can be found in an earlier draft version of the text that the Member of Parliament in charge of the whole reform brought to the negotiations in the Industry Committee which lead the work at the European Parliament:

Article 5a(7) of the report of the Rapporteur[17]:

> *"The user shall be in full control of the European Digital Identity Wallet and its own data. The issuer of the European Digital Identity Wallet shall ensure that it is built on privacy by design principle. In particular, the EDIW shall have the following features: a)* ***for issuers of the European Digital Identity Wallet it shall be technologically impossible to receive any information on the use of the Wallet or its attributes. For the purpose of protecting user data against loss or corruption, encrypted synchronization and encrypted backup functions shall be permitted, with the previous explicit consent of the user.*** *"*

Fully DPI-safeguard compliant provision that was not adopted.

RECOMMENDATION 5: NO UNIQUE PERSISTENT IDENTIFIERS

Any DPI that contains personal identifiable information has to answer how to correlate that information back to the same individual over a prolonged period of time and potentially across the boundaries of separate systems and data controllers. We usually refer to these as Person identification data (PID) and a common example is a social security number.[18] The first and simplest idea of a PID for most system architects is a Unique Persistent Identifier (UPI). Such a brute force approach basically hands out unique serial numbers for every person that stick with them for life and uniquely and persistently identify them in diverse and otherwise unconnected sets of data. Such UPI can be understood as a kind of super cookie which allows the tracking of user across all areas of life and daily interactions. From a technical point of view, it could not be easier to combine data about a person across different public sectors, companies or even when one entity obtains the personal data from another (via mergers or data breaches).

The privacy impact of a PID is directly proportionate to its prevalence. Hence, different solutions of the problem of PIDs have emerged. Sector specific PIDs create different identifiers for different branches of society like health, finance, social media, commerce, etc. Those sector specific PIDs are usually mathematically derived from a stem number, which allows the translation of sector specific UPIs where necessary. Some countries have successfully been using such a system in their e-Government for 20 years.[19] The problem arises when the DPI is opened for the private sector and sectors include data-hungry industries like social media, e-Commerce, health or finance. In these scenarios a correlation of data across relying parties in a sector has to be avoided.

Our suggestion for a safeguard in this area are Pairwise Pseudonymous Identifiers (PPIDs), which are unique for different relying parties, but opaque and random for anyone trying to correlate them across relying parties. Support for this technology can be found in NIST specifications[20] or modern standards like OpenIDConnect.

17 The leading Member of the European Parliament Romana Jerkovic proposed this text in her report on the eIDAS Regulation to the leading ITRE committee in amendment 70 and 71. https://www.europarl.europa.eu/doceo/document/ITRE-PR-732707_EN.pdf Because of the competency agreement between the ITRE and LIBE committee, this text was not in the final parliament position.

18 See also the mapping exercise of the EU-US Trade and Technology Council: https://futurium.ec.europa.eu/system/files/2023-12/EU-US%20TTC%20WG1_Digital_Identity_Mapping_Report_Final%20Draft%20for%20Comment_22122023.pdf

19 https://pure.tugraz.at/ws/portalfiles/portal/26511346/20191001_Japanese_Delegation.pdf or https://www.cs.ru.nl/E.Verheul/papers/eID2.0/eID%20PEP%201.29.pdf

20 SP 800-63C. https://pages.nist.gov/800-63-3/sp800-63c.html

In the eIDAS reform the original proposal foresaw one UPI used across the private and public sector in all cases where identification is required by law. **This proposal was clearly rejected** by the negotiators.

Article 11a of the Commission Proposal for the eIDAS Regulation[21]:

> *"(1) When notified electronic identification means and the European Digital Identity Wallets are used for authentication, Member States shall ensure unique identification.*
>
> *(2) Member States shall, for the purposes of this Regulation, include in the minimum set of person identification data referred to in Article 12.4.(d), a* ***unique and persistent identifier*** *in conformity with Union law, to identify the user upon their request in those* ***cases where identification of the user is required by law****."*

Article 12 (4) (d) of the Commission Proposal for the eIDAS Regulation[22]:

> *"a reference to a minimum set of* ***person identification data necessary to uniquely and persistently represent a natural or legal person****;"*

Non-DPI-safeguard compliant provision that was not adopted.

In the adopted legislation, the original proposal was replaced with an obligation to uniquely represent a person and a mechanism for identity matching in cross-border cases for the public sector. Examples of such cross-border public sector use cases would be justice and financial affairs in which a citizen of one country has to be uniquely identified for police or taxation reasons in another country.

Article 11a of the eIDAS Regulation:

> *"(1)* ***When acting as relying parties for cross-border services****, Member* ***States shall ensure unequivocal identity matching for natural persons*** *using notified electronic identification means or European Digital Identity Wallets.*
>
> *(2)* ***Member States shall provide for technical and organisational measures to ensure a high level of protection of personal data used for identity matching and to prevent the profiling of users.****"*

Article 12 (4) (d) of the eIDAS Regulation:

> *"a reference to a* ***minimum set of person identification data necessary to uniquely represent a natural or legal person****, or a natural person representing another natural person or a legal person, which is available from electronic identification schemes"*

Partially DPI-safeguard compliant provision that was adopted.

In an earlier version of the text from the Civil Liberties committee of the European Parliament, which had exclusive competency on data protection, the Pairwise Pseudonymous Identifiers (PPID) were proposed. This would have implemented the safeguard properly. Sadly, this text was not adopted.

21 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A281%3AFIN
22 *Ibid.*

Article 5a (4)(e) of the first reading position of the European Parliament[23]:

> *"(e) ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represents the natural or legal person and that* ***the reference to that data is different for the different relying parties****, if legally required"*

Fully DPI-safeguard compliant provision that was not adopted.

RECOMMENDATION 6: RIGHT TO PSEUDONYMITY

The wide availability of cheap technology to identify persons online or in physical proximity settings offline would foreseeably lead to the proliferation of government certified identity information in areas of life where previously anonymity was accepted. For example, the reservation of a restaurant table, the booking of a train ticket, the buying of alcoholic beverages should not require the user to transmit their identification information. Simply using the DPI for login into an online service should also not require the user to hand over their legal name and identity. Particularly vulnerable groups depend on anonymity to exercise their right to freedom of speech, freedom of political participation or be free of discrimination when conducting business. This includes in particular, people living with disabilities or suffering from mental illness, ethnic or LGBTIQ minorities and stateless people.

Therefore, the right to use pseudonyms is ensured in several provisions in the EU's DPI legislation. Critically important is that the right to pseudonymity is guaranteed also when interacting with the private sector. Only when legislation obliges the company to check the legal identity of a customer or visitor, can a right to use pseudonyms be restricted. In order to ensure unlinkability the pseudonyms need to be freely chosen by the user and stored locally so as not to allow them to be linked to the legal identity at a later stage.

Article 5:

> *"****Without prejudice to specific rules of Union or national law requiring users to identify*** *themselves or to the legal effect given to pseudonyms under national law,* ***the use of pseudonyms that are chosen by the user shall not be prohibited****."*

Article 5a(4):

> *"European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: […] (b)* ***generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;****"*

Article 5b(9):

> *"Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets.* ***Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.****"*

23 https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.docx

Recitals 19, 22 and 60 of the eIDAS Regulation:

> *"(19) [...]* ***Reliance on the legal identity should not hinder European Digital Identity Wallet users to access services under a pseudonym, where there is no legal requirement for legal identity for authentication.*** *[...]*
>
> *(22) European Digital Identity Wallets should include a functionality to* ***generate user chosen and managed pseudonyms, to authenticate when accessing online services****.*
>
> *(60)* ***Unless specific rules of Union or national law require users to identify themselves, accessing services by using a pseudonym should not be prohibited.****"*

Fully DPI-safeguard compliant provision that was adopted.

RECOMMENDATION 7: FREE AND OPEN SOURCE

A free and open source software licence is a precondition for the success of digital public infrastructure for several reasons. First, given the central role of DPI in people's lives their functioning needs to be under public scrutiny and properly understood. Without an open source licence the government would ask users to install a black box software on their devices, which would result in very understandable resistance in certain parts of society – chief among them the technical community that often drives the public debate around DPI. Secondly, open source software also offers many benefits from an IT-security perspective, since security researchers can audit the source code and help keep the systems up to modern standards. Lastly, tax-payer-financed DPIs should be under a free software licence to follow the principle of "public money, public code".[24] Since the public often pays for these systems, the benefit of their development should not be privatized. Thereby, the spread of freely licenced systems would also help their proliferation by reducing cost. Lastly, a free software licence allows for easier and decentralised adoption of these systems to accessibility requirements and for local needs in general.

The EU adopted hard obligations and soft recommendations for open source licencing of DPI components. Those are neither wholistic, nor do they fulfil the free software requirement.

Article 5a(3) of the eIDAS Regulation:

> *"The source code of the application software components of European Digital Identity Wallets shall be* ***open-source licensed****. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed."*

Recital 33 of the eIDAS Regulation:

> *"The transparency of European Digital Identity Wallets and the accountability of their providers are key elements to creating social trust and trigger acceptance of the framework. The functioning of European Digital Identity Wallets should therefore be transparent and, in particular, allow for verifiable processing of personal data. To achieve this, Member States*

24 https://publiccode.eu/en/

*should disclose the source code of the user application software components of European Digital Identity Wallets, including those that are related to processing of personal data and data of legal persons. T**he publication of this source code under an open-source licence should enable society, including users and developers, to understand its operation, audit and review the code. This would increase users' trust in the ecosystem and contribute to the security of European Digital Identity Wallets by enabling anyone to report vulnerabilities and errors in the code.** Overall, this should provide suppliers with an incentive to deliver and maintain a highly secure product. However, in certain cases, the disclosure of the source code for the libraries used, communication channel or other elements that are not hosted on the user device, could be limited by Member States, for duly justified reasons, especially for the purpose of public security."*

Recital 22 of the COVID-19 Certificate:

*"[...] The infrastructure should be developed, with a **strong preference for the use of open-source technology**, to function on different major operating systems, while ensuring that it is protected from cybersecurity threats. [...]"*

Partially DPI-safeguard compliant provision that was adopted.

RECOMMENDATION 8: PRIVACY COCKPIT

A DPI should have a full transaction history of every request for information the user has received, the identity of the relying party issuing the request and the information the user has shared with them. Furthermore, the DPI should offer the possibility to request the deletion of any personal data from the records of the relying party and also to file a complaint about them with national regulatory authorities. This includes a requirement of the relying party to always identify themselves to the user before requesting any information from them.

Article 5a(4) of the eIDAS Regulation:

*"European Digital Identity Wallets shall enable the user, in a manner that is **user-friendly**, transparent, and traceable by the user, to:*
[...]
*(d) **access a log of all transactions** carried out through the European Digital Identity Wallet via a common dashboard enabling the user to:*
*(I) view an **up-to-date list of relying parties with which the user has established a connection** and, **where applicable, all data exchanged**;*
*(ii) **easily request the erasure by a relying party of personal data** pursuant to Article 17 of the Regulation (EU) 2016/679);*
*(iii) **easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received;**"*

Article 5a(5) of the eIDAS Regulation:

"European Digital Identity Wallets shall, in particular:
(a) support common protocols and interfaces:

[...]
*(ix) for **requesting a relying party the erasure of personal data** pursuant to Article 17 of Regulation (EU) 2016/679;"*

Article 5b(8) of the eIDAS Regulation:

"Where relying parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the user."

Fully DPI-safeguard compliant provision that was adopted.

RECOMMENDATION 9: NO REQUIREMENT FOR BIOMETRICS

Using biometric authentication or identification methods should not be a precondition for using DPI systems. Biometric systems contain unique risks that require them not to be mandatory barriers for accessing the DPI system. All forms of biometrics have a high risk in case of data breaches and also exclude people that lack the physical characteristics which are the input of the biometric system. For example, lack of eyes, limbs or unreadable fingerprints because of hard manual labour.

Furthermore, if biometric information is stored this should happen per default on the device of the user. Many modern smartphones hold biometrical information for authentication only in the secure enclave of the device and never upload it onto the cloud. Central storage of biometrical information requires the explicit consent from the user, which means a consent that is always optional and can never be tied to the functioning of the service itself.

The European Parliament adopted a great text enshrining such a requirement:

Recital 11 of the first reading mandate adopted by the plenary of the European Parliament on the eIDAS Regulation[25]:

*"European Digital Identity Wallets should ensure the highest level of security for the personal data used for identification and authentication irrespective of whether such data is stored locally, in decentralised ledgers or on cloud-based solutions, and taking into account the different levels of risk. **Using biometrics to identify and authenticate should not be a precondition for using European Digital Identity Wallets**, notwithstanding the requirement for strong user authentication. **Biometric data used for the purpose to authenticate a natural person in the context of this Regulation should not be stored in the cloud without the explicit consent of the user.** Using biometrics is one of the identifications methods providing a high level of confidence, when used in combination with 'what you know' factor. **Since biometrics represents a unique characteristic of a person, the use of biometrics should not be obligatory**. Furthermore the use of biometric data should be limited to specific scenarios pursuant to Article 9 of Regulation (EU) 2016/679, and requires organisational and security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with Regulation*

25 https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html

2016/679. ***Storing information from European Digital Identity Wallets in the cloud should be an optional feature only active after the user has given explicit consent.*** *Where European Digital Identity Wallets are issued on a personal electronic device of the user, their cryptographic material should be, when technologically possible, stored in the secure elements of European Digital Identity Wallets."*

Fully DPI-safeguard compliant provision that was not adopted.

Sadly though, the adopted text by the European legislators no longer contains any reference to biometrics. While its important to state that there is no mandated biometrics for any DPI, the text also no longer prevents biometrics to be a precondition for DPI.

Recital 30 of the eIDAS Regulation:

"European Digital Identity Wallets should ensure the highest level of data protection and security for the purposes of electronic identification and authentication to facilitate access to public and private services, irrespective of whether such data is stored locally or on cloud-based solutions, taking due account of the different levels of risk."

Non-DPI-safeguard compliant provision that was adopted.