# How does the EU Digital Identity Wallet change the risk of over-sharing data? A Dutch perspective.

Henk Marsman[1] Michael Klenk[2], Mark de Reuver[2], Nitesh Bharosa[2]

[1] *Independent researcher, Leiden, The Netherlands*

*2 Delft University of Technology, Jaffalaan 5, Delft, 2628 BX, the Netherlands*

**Abstract**

The European Union (EU) Digital Identity Wallet (DIW) intends to give citizens control over personal data sharing. The DIW users will have full and sole control over their data. The EU intends to address the risk to citizens' privacy in cases where data from and about users is gathered and exchanged by online service providers. However, it is unclear how users of the EU DIW can decide what data to share and how to prevent sharing too much data with online service providers. In order to reduce this risk, we need to understand it first. Drawing on expert interviews, this paper presents a novel analysis of the risk of over sharing through the EU DIW. It defines the risk and what aspects influence the risk from literature, documentation and expert interviews. Over-sharing data occurs when users share more data than strictly required for the service or product acquired online and multiple aspects influence this risk, specifically the user capabilities and orientation, the loss of context awareness, the quality of the data and the ease of sharing.

**Keywords**

eIDAS, digital identity wallet, data, privacy, over-sharing

## 1. Introduction

Users share data online to obtain a wide variety of services and products. How organizations use this data and how users have gone from consumer to product has been widely studied in academia. Examples include literature on privacy and related business models [1], literature on the regulation on data protection (like GDPR [2]), and privacy decision making [3]. Minimizing data sharing to protect user interests is discussed in the literature on online privacy, and cases such as Facebook and Cambridge Analytica have shown how data is gotten from and used to influence individuals [4].

To provide citizens of European Union EU (EU) Member States (MSs) with the means to control where they share data with both public and private organizations the EU Digital Identity Wallet (DIW) is described in the amended eIDAS Regulation [5]. The DIW gives

*Proceedings EGOV-CeDEM-ePart conference, September 1-5, 2024, Ghent University and KU Leuven, Ghent/Leuven, Belgium*

EMAIL: throughidentity@proton.me (A.1), m.b.o.t.klenk@tudelft.nl (A.2), g.a.dereuver@tudelft.nl (A.3), ), n.bharosa@tudelft.nl (A.4)

ORCID: 0000-0003-3291-1506 (A.1), 0000-0002-1483-0799 (A.2), 0000-0002-6302-7185 (A.3), 0000-0002-3919-6413 (A.4)

users full and sole control to decide where they share data. This raises the question of whether users can bear that responsibility or if they risk sharing too much of their data online [6], [7]. Before measures can be identified and implemented to support the user in online data-sharing decision-making, we need to understand better how the DIW impacts data-sharing online and how the DIW changes the risk of over-sharing data. Given the emerging nature of the DIW, hardly any research sheds light on this risk of over-sharing. To detail the risk and impact experts from the Dutch context were interviewed.

This short paper describes in the second section the background and literature review, the third section describes the research methodology, the fourth and fifth sections present the results of analysis and expert interviews, and a conclusion in section six.

## 2. Background

The European Union has recognized the need for trust in online interactions since the early days of the Internet. National eID schemes appeared as early as the 1990s and have been studied from an identity model perspective [8], [9] and the actual implementations and their status per country [10], [11], [12]. Recently the EU Regulation on cross-border use of national eID solutions was amended and the Digital Identity Wallet (DIW) is introduced as the solution for online identification and sharing of data [13]. The DIW has multiple goals, including online authentication, electronic signing, and control over personal data. This should enhance privacy, legal certainty and trust in online interactions. Citizens of EU Member States can use the DIW to access and share their data in all EU Member States with public and private sector organizations [14], detailed in the Architecture and Reference Framework (ARF) [15].

As a solution, digital wallets themselves are not new, the earliest appeared over a decade ago at Bigtech companies, in 2021 counting at least 18 wallet suppliers [16]. The EU DIW differs from the existing digital wallets by being regulated on European level and storing national digital identifying data for citizens. In addition, the DIW is subject to strict oversight, it needs to be offered free of charge to the user, and the code needs to be open source. Specific private sector industries are required to accept the DIW.

### 2.1. Sharing data with the EU DIW

Sharing data with the EU DIW starts with the user interacting with a Wallet Provider (WP) to install a nationally certified (eIDAS compliant) wallet on their device. With the wallet the user interacts with Issuing Parties (IP) to retrieve data and store it in the wallet, often starting with their 'digital passport', the Person Identification Data (PID). Then the user interacts with Relying Parties (RPs) where they share data (identifying data to login or other data). The user of the DIW has full and sole control over what data is stored and what data is shared.

IPs can be governmental institutions, issuing national identity, diplomas or driver licenses; or private organizations, issuing other credentials. RPs under eIDAS Regulation can be public online service providers of every Member State and organizations in industries including transport, energy, financial services, social security, health, postal services, education and others that face strong customer authentication requirements, per

article 6db of the Regulation. How these actors interact is detailed in the ecosystem description, overview and roles in the ARF [15]. Data can be shared by the user with the wallet when and where needed, reducing the need for centralized data stores (that can be breached). The IPs and RPs do not communicate to exchange user data, as is often the case now, reducing their awareness of what user has been engaging online where, reducing profiling and tracking risks for the user.

Illustratively the Dutch Example Wallet developed by the Dutch EDI program presents the user a series of questions when sharing data online [17]. These questions include confirmation of the RP, the data shared (including rationality for each data element and the related data agreement) and confirmation by PIN. Upon approval the wallet presents a confirmation screen, and the logging records the sharing of data to this RP.

## 2.2. Review of literature and public documentation

Users share online data with service providers to use services and products. In the current interactions, over-sharing of data already occurs in forms where users are requested to submit their data (for example in webforms). Users decide, consciously or not, to submit their data. When users share data there is the risk that they share more data than necessary to provide the service and there is the risk that the data is used for other purposes than it was initially shared for. The data could be sold and could become an ingredient of a business model that sees users as a product and not as a user, [1]. In order to decide where to share personal data, and where not, users make a privacy decision for which they need to understand the context of the (data) transaction, the value of their data, the benefit(s) they obtain by sharing it, and the future consequences of shared data. When users are unaware they are making a privacy decision, or not sufficiently able to do so, they may over-share.

Users may over-share data when the user has limited or no alternatives to obtain the service. There is a power imbalance between the user and the service provider that impacts how freely the user can consent or deny, [18]. Users may not have the necessary expertise on technical and legal matters and still need to make decisions on data sharing, [19]. Not fully understanding the impact of data sharing or possible future consequences increases the risk that the user shares more data than needed. Users can be misled to share data or simply just don't care and share, [6], [7].

The Dutch government identifies the risk of over-sharing as part of their activities to work on a digital identity solution for eIDAS [20]. Over-sharing is impacted by unclarity with users regarding which data is shared for what purpose and with whom, [21]. Other barriers to the use of the wallet that impact the risk of over-sharing are the low digital readiness of citizens and vulnerable or (over)confident users [22]. The related loss of context-awareness when sharing, and the lack of gatekeepers that are present in centralized or federated identity and data-sharing models contribute to the risk of over-sharing [6]. The user interface and how the user is presented with data-sharing requests contributes to over-sharing when dark patterns, user interfaces that trick or manipulate users into taking certain actions [23], are used to steer individuals to over-sharing of data [7]. And when personal advertisements finance the business model of the RP this adds to the risk of over-sharing, since these RPs may ask users to share more data than needed, [24].

## 3. Research Methodology

This ongoing research paper uses literature study and review of publicly available documentation on eIDAS and the DIW. The initial definition from the risk of over-sharing is taken from Dutch policy documentation and expanded by the analysis of literature and documentation. Because no other MS have been known to identify this risk of over-sharing the research starts with a focus on the Dutch context, where this risk is identified, and this also gives a coherent perspective from one EU MS and its activities.

To validate the analysis and expand the description of the risk 16 experts are interviewed. Each interview consisted of 7 questions on the risk of over-sharing data with the EU DIW and had a duration on average of 30 minutes. The interviews are conducted online, in a semi-structured way. The transcripts from the interviews are analyzed with a focus for this paper on the responses to the question on what the risk of over-sharing is with an EU DIW (question 1). The full list of questions is included in the Appendix.

The 16 experts are selected from Dutch organizations that play a role in the EU DIW. These include 4 policy makers and experts working at the Dutch government or public institution, 6 from digital wallet providers, 4 from Relying Parties that have users that share data from digital wallets and 2 representatives from interest groups representing privacy interest and the interests of minors as a specific group in the population. All interviewees have expertise and are involved in current digital wallet and / or EU DIW activities.

The Issuing Party and the User, also actors in the EU DIW ecosystem, are not included in the interviews because respectively the focus is on sharing data (not acquiring data) and what experts view is (not general audience or specific users). The risk of over-asking and of over-sharing is considered in this paper as two sides of the same coin, although in future research for this ongoing research they may also be investigated as distinct events.

The research presented in this paper is subject to several limitations. The research is limited to the Dutch context and expanding this context (to other geographics / EU Member States) may lead to different perspectives, especially from interviews. The research is the result of only a high-level analysis of part of the interview results, and a deeper analysis will yield a richer result with more insights. The research addresses the perspectives of four types of experts on the risk of over-sharing. Expanding this to more perspectives with experts from other disciplines, such as experts in consumer behavior, will add to what consumers actually are capable of. The impact of regulation such as the GDPR as a context to data sharing impacts the use of the EU DIW has not been included in this research but is expected to also have impact.

## 4. Aspects of the EU DIW impacting the risk of over-sharing data

The analysis based on the literature and description from public documents how the EU DIW is designed to function provides a list of aspects that impact the risk of over-sharing data:

- Users have full control over what data they store in the DIW, and with whom they share this data. This means that safeguards from other actors or institutions in the

actual decision to (over) share data are not available and the user needs to carry the responsibility, where currently data and identity providers protect data as well.

- The wallet will increase the ease-of-use for sharing data ('one swipe' or just a few 'accepts' in the wallet). Easier data sharing can lead to over-sharing.
- The data includes verified attributes with a high level of assurance, such as legal identifying data for the users' nationality, similar to the national eID solution, and financial and medical information. Sharing this data in scenarios where previously the user would provide self-acclaimed data constitutes over-sharing.
- The EU DIW can be used to share data with public online services, private sector services and very large online platforms. The use is not restricted to EU service providers or context. The user may not be aware of the context when sharing data online, where the data would not have been shared in the offline context.

## 5. Results of expert interviews

Experts were interviewed and asked to define the risk of over-sharing and reasons for why it could occur. The risk of over-sharing data is defined as 'sharing more data than is required for the service or product that the user wants to obtain'. This definition includes sharing sensitive data, such as personal identifiable information or medical information, and data that is subject to regulation (such as the Dutch citizen ID, when it is not allowed

The experts provide a list of aspects of the EU DIW and reasons for why the use of the EU DIW changes the risk of over-sharing data. These are:

- The desire of the user to obtain a service or product can result in a less critical evaluation by the user of the data sharing request, or simply accepting any data sharing request presented. Once a user has decided they want to get a service or product their 'goal orientation' makes that anything that stands in the way of that goal can be perceived as something that 'has to be overcome', including sharing any data that is required to obtain that service. Users then just click 'OK' without evaluating the request.
- Users are often unaware of what data is being shared and with whom. Users simply do not comprehend that they are sharing data and what data it is they are sharing. Users are also not sufficiently aware of the future consequences of shared data.
- Not being able to determine what is appropriate data to be shared for a specific service increases the risk of over-sharing because the user cannot assess whether the Relying Party (RP) is over-asking. The user may decide to share the data also in cases where factually not all data is required for the service.
- The wallet allows users to share data across many contexts. This may lead to over-sharing data when the user assumes trust from a known context in a different context or discards evaluations made in the other context and shares the data.
- The ease of sharing data increases the risk of over-sharing. When the user is in a hurry ('haste') or distracted the wallet makes it so easy to share data that the user can share the data before even realizing what they are doing. RPs may make use of this feature to reduce friction in the customer journey.

- Qualified data in the wallet may increase the risk of over-sharing. Where the user may have previously submitted partial or false information in webforms, this is now more difficult (or even impossible). The wallet holds qualified data that is issued (verifiably) by a specific Issuing Party and with a specific level of assurance (trust). This makes it difficult to 'lie' about oneself online.
- Request fatigue results from many requests to share data, leading the user to simply accept every request. The user can suffer from fatigue or simply be annoyed by the many requests. Clicking 'yes' to every request is also labelled as 'habitual accepting' and is compared to the current user evaluation of cookie consent walls.
- Influencing and manipulation of the user to share data can lead to increased risk of over-sharing data with a RP. Cases of Facebook show that emotional influencing can change data sharing behavior. Users can be seduced or nudged to over-share data. Dark patterns can be applied to influence users to share more data.
- A RP business model that is driven by data gathering and selling for profiling and (aggressive) advertising campaigns may cause the RP to over-ask and increase the risk of over-sharing. Experts expect that 'data-hungry' RPs will over-ask.
- Data requests that contain separate data elements but only can be approved as a whole increase the risk of over-sharing. With only a yes/no response available for the entire data set and no nuancing the user shares all the data and may over-share.

Experts noted that over-sharing data with a digital wallet is a realistic risk, although over-sharing data as a risk is not a novelty.

## 6. Conclusion

In summary we conclude that aspects of digital wallets and, specifically the EU DIW impact the risk of over-sharing data, detailed by experts as expansion of the first analysis.

Over-sharing data is impacted by the goal orientation of the user and the awareness and knowledge, both in general and for assessing the proportionality of data requests. This is furthermore complicated by the cross-context sharing of data and the ease of sharing data. Users may be subject to influencing techniques (including manipulative techniques) and experience request fatigue. Having qualified data to share increases the impact of over-sharing and also makes them a more interesting target for 'data-hungry' relying parties. When data requests cannot be unbundled the risk of over-sharing is also affected.

The EU DIW changes the risk significantly. With a better understanding of the risk and its influence, future research into mitigating measures can be more specific and effective. Future publications from this research will report on user capabilities and mitigating measures for various actors in the data wallet ecosystem.

## Acknowledgements

We acknowledge the time and input given by the interviewees and the time granted by SonicBee B.V. to work on this research. We thank the reviewers for their valuable comments

and suggestions, which helped us improve the quality of the paper. No funding was received for this research.

## References

[1] S. Zuboff, “Surveillance Capitalism and the Challenge of Collective Action,” New Labor Forum (2019): 10-29.

[2] European Commission, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation),” 2016.

[3] A. Acquisti and J. Grossklags, “What can behavioral economics teach us about privacy,” *Digital privacy: theory, technologies and practices*, (2007): 363-377.

[4] D. Susser, B. Roessler, and H. Nissenbaum, “Online manipulation: Hidden influences in a digital world,” *Geo. L. Tech. Rev.* (2019): 1.

[5] European Parliament, “European Parliament legislative resolution (…) amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.” 2024. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.html

[6] J. Doesburg, B. P. F. Jacobs, and H. K. Schraffenberger, “Measures against over-asking in SSI and the Yivi ecosystem,” (2023).

[7] B. Jacobs and H. K. Schraffenberger, “Friction for privacy: Why privacy by design needs user experience design,” (2020).

[8] Modinis IDM Study Team, “Study on identity management in eGovernment: Common terminological framework for interoperable electronic identity management,” 2005. URL: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc

[9] H. Kubicek, “Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries,” Identity in the Information Society, (2010): 5–26. doi: 10.1007/s12394-010-0052-0.

[10] Modinis IDM Study Team, “Study on Identity Management in eGovernment: The Status of Identity Management in European eGovernment initiatives,” (2006). URL: https://www.cosic.esat.kuleuven.ac.be/modinis-idm

[11] H. Kubicek and T. Noack, “Different countries-different paths extended comparison of the introduction of eIDs in eight European countries,” Identity in the Information Society (2010): 235–245. doi: 10.1007/s12394-010-0063-x.

[12] U. Melin, K. Axelsson, and F. Söderström, “Managing the development of e-ID in a public e-service context,” Transforming Government: People, Process and Policy (2016): 72–98. doi: 10.1108/TG-11-2013-0046.

[13] European Commission, “Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 (…),” (2021). URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910

[14] A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, F. A. Marino, and S. Ranise, “The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes,” Applied Sciences (2022).

[15] E. C. eIDAS Expert Group, "European Digital Identity Wallet Architecture and Reference Framework v1.4.0." (2024). URL: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v1.4.0/docs/arf.md
[16] C. van Ramshorst, L. Kluiters, and S. den Breeijen, "SSI Speelveldanalyse," (2021): 1–61, URL: https://www.rijksoverheid.nl/documenten/rapporten/2021/10/01/eindrapport-nederlandse-self-sovereign-identity-ecosysteem-ssi
[17] M. van B. Z. EDI programma, "Release Digitale Identiteit Wallet Realisatie." (2024). URL: https://www.figma.com/design/WhKRswMoKDde7w5VhXCEcy/20240319_Release_Digitale-Identiteit-Wallet_Realisatie
[18] N. Martin, "The Chimera of Control Some Critical Reflections on Self-Sovereign Identity," (2023). URL: https://www.sdika.de/]
[19] C. Lazaro and D. Le Metayer, "Control over personal data: True remedy or fairy tale," (2015).
[20] A. C. van Huffelen, "Waarden, kansen en uitdagingen rond het Europese Digitale Identiteit raamwerk," (2022). URL: https://www.rijksoverheid.nl/documenten/brieven/2022/07/26/waarden-kansen-en-uitdagingen-rond-het-europese-digitale-identiteit-raamwerk
[21] B. Lukkien, N. Bharosa, and M. de Reuver, "Barriers for Developing and Launching Digital Identity Wallets," EasyChair (2023).
[22] M. Hünseler and E. Pöll, "Promises and Problems in the Adoption of Self-Sovereign Identity Management from a Consumer Perspective," IFIP International Summer School on Privacy and Identity Management (2022):. 85–100.
[23] J. Luguri and L. J. Strahilevitz, "Shining a Light on Dark Patterns," Journal of Legal Analysis (2021): 43–109. doi: 10.1093/jla/laaa006.
[24] A. Terpstra, A. Graßl, and H. K. Schraffenberger, "Think before you click: how reflective patterns contribute to privacy (Position Paper)," (2021).

## A. Appendix: Interview Questions

The interviews are semi-structured with these questions on the EU DIW.

1. How would you word the risk of over-sharing data? (risk and consequences)
2. Which scenario's (situations) could include an over-sharing of data?
3. What characteristics contribute to over-sharing of data for a) the user, b) the wallet and c) the Relying Party?
4. What capabilities do users need to be able to share the data (only) where they want to?
5. To what extent do you expect that users have these capabilities?
6. What are measures that can be taken to provide users with more capabilities?
7. Which actors should be responsible for (taking) these measures?