Lukasz Olejnik, PhD
https://lukaszolejnik.com

Written contribution.

Privacy and data protection assessment of the "*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 2021/0136(COD)*"

This assessment is prepared in response to a request by the LIBE Secretariat in the name of the MEP Cristian Terhes (rapporteur of eID file; requested on 19.01.2022). The focus of this assessment is data protection and privacy. Although (also including the timing of the request) it is a holistic view, the aim is to be sufficiently thorough, and complete. It is not the intention of this report to duplicate any other opinions already existing. While this assessment is limited to eID, it also considers practical issues, including future oversight, deployment, etc.

This work is submitted with total independence, and it was in no way affected by the dealings or writings of any external factor.

1. It is hard to notice that the Regulation (EU) No 910/2014 was far from successful in establishing broad access to electronic identification (eID).
2. The new proposal for a Regulation aims to change this situation, giving Europeans access to electronic identity. In doing so, it would introduce several security, privacy, and data protection challenges, including due to the interoperability and standardisation needs.
3. The privacy and data protection standards should be grounded in Regulation (EU) No 2016/679 (the GDPR) [*as noted in Recital 6*].
4. Recital 10 highlights the needs for security ("*pursuant to Regulation (EU) 2019/881*") and data protection certifications ("*pursuant to Regulation (EC) 2016/679*"). No such suitable standards seem to exist. Competent authorities must work towards establishing them, and contingency plans must exist until mature schemes of the kind are defined. Furthermore, it will be challenging to find a common compromise between the two regulations (2019/881 and 2016/679) if the competent authorities would choose not to work in a synchronised manner. For this reason, they should closely cooperate from the start. Similar comments are issued concerning the devoted Article 6c.
5. In Recital 11, the sentence "*European Digital Identity Wallets should ensure the highest level of security for the personal data used for authentication*" is at best meaningless. It has no content. The sentence following it, and

referencing the use of biometry even undermines it. This recital should be rewritten (split in two). Furthermore, in line with Regulation 2016/679 and its Article 9(1), the use of biometry in eID means the processing of special categories of data, even if it may be legally justified in line with Article 9(2).

6. The preceding points strongly suggest that there should be a mandatory data protection impact assessment (DPIA, Regulation 2016/679 Article 35) conducted for each part of the system, as well as a general one for the entirety of the system. This DPIA should be made public to contribute to the building of public trust.
7. In Recital 18 it is remarked that "*In line with Directive (EU) 2019/882 22 , persons with disabilities should be able to use the European digital identity wallets, trust services and end-user products used in the provision of those services on an equal basis with other users*". It must be understood that the privacy and data protection challenges linked to persons with disabilities may be specialised. Including considering the level of the user interface, enrollment, etc. This should be clarified in the Recital. Furthermore, it must be borne in mind that any potential to misuse the eID system against persons with disabilities can cause problems to such persons, for example in terms of explaining the misuses or correcting/alleviating the problems (for example in a situation when the eID is abused to forge a signature). This Regulation should explicitly stipulate the need for special cases and modes of operation that include the needs of persons with disabilities, including the breach incidents affecting such persons. While this may be clarified on the level of the DPIA, in practice the persons tasked with making the DPIA may ignore this problem, or the DPIA may leave much to desire. For this reason, it should be explicitly demanded for in the Regulation. This topic is also mentioned in Article 6a(10), but please note that Directive 2019/882 does not consider any specific risks identified. The stipulations of Article 15 are also not sufficient. The details, including the required standards, should be the task of a designated body/institution. The Regulation must directly task a particular unit with the needs to prepare such standards. Mentioned as currently is, it is left to be done in undefined ways, by undefined parties.
8. In Recital 23: "*In cases where the supervisory body under this Regulation is different from the competent authorities designated under Directive XXXX/XXXX [NIS2]*". The Regulation should consider stipulating that the responsible competent authorities should be the same.
9. The **sources of trust** and intermediaries mentioned in Recitals 30, 31 (etc) should all respect the need to monitor and guarantee the highest level of cybersecurity, privacy, and data protection.
10. In Recital 32: "*web-browsers should ensure support and interoperability with Qualified certificates for website authentication pursuant to Regulation (EU) No 910/2014. They should recognise and display Qualified*

certificates for website authentication". This requires common web standards of aspects related to things such as the handling, processing, displaying of certificates. Lawmakers should appreciate that the preparation of such technical standards, and their deployment, would take time, but more importantly, it could lead to potential and actual negative impact on security and privacy of web users. Support should not be required.

11. Consider removing Recital 34, the use of ledgers and blockchain-like technology in terms of privacy and data protection is currently underexplored (also in line with Regulation (EU) 2016/679), and it may undermine the trust in eID. Furthermore, it currently is not clear why electronic ledgers should be used in the eID system, considering the privacy and data protection needs. It is certainly not explained sufficiently, but simply included as-is.
12. Concerning Article 5 ("*the use of pseudonyms in electronic transactions shall not be prohibited…*"), the term *'pseudonym'* is undefined (e.g. in Article 3). For example, is it linked in any way to the 'pseudonymisation' as used in Regulation (EU) 2016/679? This must be clarified.
13. In Article 6a(7): "*The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services*". It should also be defined that the collected information is deleted when not needed: after a time as defined in the DPIA documents prepared. Such a time period may be stipulated in the Regulation itself. It should not exceed two years, possibly even a month?
14. In Article 10a "*Security breach of the European Digital Identity Walles*" it should be borne in mind that security and data protection breaches must also be communicated to the competent authorities, and possibly (following a risk assessment) to the data subjects concerned. For transparency purposes, the legislator should consider making information concerning any incidents, always public. For the purposes of building public trust in the system. Article 10a must also contain a clause that *'it is without prejudice to Regulation (EU) 2016/679'* and its data breach standards.
15. Concerning Article 12b, it should be stipulated that authentication using the eID solution against a system of a "*very large online platforms as defined in Regulation [DSA] Article 25.1*", no unnecessary information should be provided in the process. In other words, the act of authentication should fully support the 'data minimisation' principle.
16. Any EC-issued implementing acts, or EC-issued technical and operational specifications (as mentioned e.g. in Article 6b(4)) warrant separate security, privacy, and data protection assessments, possibly including separate DPIAs. This should be clarified in this regulation.
17. Systemic risk assessments should be established by competent authorities and should include misuse case studies/scenarios.

18. It should be understood that the matter introduced in Article 45 ("*Qualified certificates for website authentication*") is very sensitive concerning freedom of expression, security, and privacy. The risks of technical censorship capabilities must be reevaluated to avoid the mistaken introduction of certificate infrastructure that would jeopardise fundamental rights and freedoms. Specifically, it would be a shame if the EU deployed[1] censorship-supporting certificate system. It is also clear that **the introduction of such mandatory certificates may undermine web security**. It is imaginable that web browser vendors would actively fight[2] the introduction of such capabilities. Furthermore, it is possible that undermining of web security could negatively impact the Digital Single Market. This is likely not the intention of the EU lawmakers.
19. Members of the European Parliament should consider whether they desire legislation potentially introducing such infrastructures. It should first and foremost be considered whether such a system is in line with European values[3], unless, perhaps, it conforms to other value sets, subscribed to in very different countries in other geographic placement. Members of the EP should then decide accordingly, considering their priorities, and the priorities of European citizens.
20. Article 45 of the preceding eID Regulation was a failure. The current regulation project plans to build on this failure, and possibly take it to the next level. The net result may potentially be an extra level of failure. It is unfortunate that this may come at the expense of user security, and in fact, the potential construction of technical censorship infrastructure ingredients. These points were not considered in the EC-issued impact assessment. This undermines their quality and credibility, including in other areas.
21. Fortunately, the fix is simple: Article 45 should consider that it is an opt-in capability, without the need to recognise such certificates. Alternative is to delete Article 45 completely: as it currently stands, it subscribes to 2000s ways of thinking about cybersecurity, while today it is the 2020s, with standards and thinking evolved. In this way, it would not be necessary to implement this functionality. The fundamental premise is that if web security standards are jeopardised, privacy and data protection cannot be sustained nor guaranteed, in any conceivable way. To introduce extra future-proof stability, a recital could further clarify the matter, again reaffirming that such certificates should not be mandatory.

22. This assessment identifies significant risks to privacy, data protection, the protection of disabled persons, as well as the general web security and cybersecurity standards in the European Union.

---

[1] https://www.gov.kz/memleket/entities/mdai/press/news/details/132113?lang=ru
[2] https://blog.mozilla.org/netpolicy/2020/12/18/kazakhstan-root-2020/
[3] Andersdotter, A., & Olejnik, L. (2021). Policy strategies for value-based technology standards. *Internet Policy Review*, *10*(3), 1-26.

23. The eID Regulation update should be updated to be in line with GDPR, but also contain more precise stipulations.
24. Lastly, it would be a shame if one additional side-effect of the Regulation (Article 45[4]) would introduce a technical censorship infrastructure, although this point goes beyond the restricted scope of privacy and data protection assessment.

About the author
Dr Lukasz Olejnik is an independent researcher and consultant dealing with cybersecurity and privacy. He authored various papers, reports, assessments.
He holds a PhD in Computer Science (Privacy) from INRIA, is a former member of the World Wide Web Consortium (W3C) Technical Architecture Group (TAG), and previously worked at and with many entities, including the European Data Protection Supervisor, the International Committee of the Red Cross in Geneva, was associated with University College London, Princeton's Center for Information Technology Policy, Oxford's Centre for Technology and Global Affairs.

Some of his most recent (2021) works considering privacy of relevance:

- Andersdotter, A., & Olejnik, L. (2021). Policy strategies for value-based technology standards. *Internet Policy Review*, *10*(3), 1-26.
- Dimova, Y., Acar, G., Olejnik, L., Joosen, W., & Van Goethem, T. (2021). The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion. *Proceedings on Privacy Enhancing Technologies*, *3*, 394-412.

[4] Please note that the clause "shall be recognised" (as to the certificates) functionally means "shall not be rejected", and in this case the technical system becomes mandatory.