H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 185

Data Protection Impact Assessment in Identity Management With a Focus on Biometrics

Tamas Bisztray[1], Nils Gruschka[2], Vasileios Mavroeidis[3], Lothar Fritsch[4]

Abstract:

Privacy issues concerning biometric identification are becoming increasingly relevant due to their proliferation in various fields, including identity and access control management (IAM). The General Data Protection Regulation (GDPR) requires the implementation of a data protection impact assessment for privacy critical systems. In this paper, we analyse the usefulness of two different privacy impact assessment frameworks in the context of biometric data protection. We use experiences from the SWAN project that processes four different biometric characteristics for authentication purposes. The results of this comparison elucidate how useful these frameworks are in identifying sector-specific privacy risks related to IAM and biometric identification.

Keywords: data protection, privacy, impact assessment, GDPR, DPIA, identity management, biometrics

1 Introduction

Managing digital identities involves the storage and processing of *personally identifiable information* (PII), i.e., data that link to individuals and can reveal confidential information such as name, address, date of birth etc. Biometric identifiers are PII and is a general term for describing a measurable physiological or behavioral characteristic of a person. Misuse of biometric data can have severe consequences [Ca13], such as identity theft or customer profiling. The European *General Data Protection Regulation* (GPDR) [Eu16] allows the processing of biometric data only under specific conditions, and it recommends conducting a *Data Privacy Impact Assessment* (DPIA).

The purpose of a DPIA is the evaluation of the activities related to data processing with respect to possible privacy risks (e.g., disclosure). Our research has identified two limiting factors applicable to DPIAs in the context of their usage. First, the GDPR does not provide any recommendations as to which of the available DPIA methods is preferred or any meaningful categorization of them. Second, privacy risks identified by the GDPR or a DPIA

[1] University of Oslo, Department of Informatics, Oslo, Norway tamasbi@ifi.uio.no
[2] University of Oslo, Department of Informatics, Oslo, Norway nilsgrus@ifi.ui.no
[3] University of Oslo, Department of Informatics, Oslo, Norway vasileim@ifi.uio.no
[4] Karlstad University, Dept. of Mathematics and Computer Science, Karlstad, Sweden Lothar.Fritsch@kau.se

are mostly generic and do not necessarily address risks applicable to particular sectors or technological domains. Although for some applications domain or sector-specific DPIA methodologies have been introduced, like RFID technologies [Eu11] and smart grid systems [Sm09], most of the existing widely-used methodologies are context independent. Thus, their use in different technological and sector-specific applications needs to be further studied.

This paper analyzes the usefulness of two different DPIA methodologies for the domain-specific use case of biometric authentication. First, we compile two lists of privacy requirements specific to IAM and biometric authentication. Second, we analyze and compare the adequacy of two widely used DPIA methodologies in assessing the privacy of the identified requirements by performing a DPIA on a biometric system and validating the results.

The paper is organized as follows. Section 2 provides background information on DPIA and the GDPR in the context of biometric authentication. Section 3 presents related work. Section 4 presents privacy requirements. Section 5 maps the identified requirements to two DPIA methodologies with the help of a concrete use case in biometrics. Finally, Section 6 discusses the results of the analysis conducted.

2 Background on Data Protection

The General Data Protection Regulation (GDPR) [Eu16] is the current privacy and data protection regulation in the European Union (including Norway, Liechtenstein, and Iceland). Of particular importance when processing data is Article 35 *Data protection impact assessment* that describes how a data controller should carry out a data protection impact assessment (DPIA) when the processing is likely to result in a high-risk related to the rights and freedoms of natural persons (data subjects). The GDPR does not provide an exhaustive list of high-risk processing operations that require a DPIA, but gives some examples within Article 35, such as *automated processing including profiling* and *personal data relating to criminal convictions and offences*.

Part of the recommendations of *Article 29 Working Party* (WP29) [Ar17] is a list of nine criteria that can be used for identifying processing operations that are likely to result in a high-risk, such as *evaluation or scoring for profiling*, and *automated decision making*. In such cases, a DPIA is recommended. It is worth mentioning that criterion 8 of WP29 is of high relevance to this research as it remarks on the potential high-risk involved when processing data for innovative use or for applying technological solutions, like in cases where multiple biometric modalities are combined for improved physical access control (e.g., fingerprint and face). The use case analyzed in this paper handles four different biometric modalities (face, iris, voice, and fingerprint) for the purpose of providing advanced biometric authentication technology in smartphone applications, such as online banking.

Article 35 specifies that a DPIA is required in cases where a type of processing is done with regards to new technology. In the context of this paper, the aforementioned is directly applicable since our use case develops innovative biometric technologies for identity and access management (IAM). What is considered to be biometric data is defined in Article 4(14). However, defining what is considered or not as new technology could be difficult to determine; thus, the general recommendation of GDPR is that in uncertain cases one should always consult the supervisory authority for recommendations. Since national-level regulations should not establish weaker criteria than the sophisticated GDPR, it is essential to review what GDPR includes about a specific topic. The Norwegian supervisory authority only requires a DPIA when biometric data is processed for identification purposes and when it is in conjunction with at least one additional criterion, whereas, Article 9(1) of GDPR clearly states that processing of biometric data for the purpose of uniquely identifying a natural person shall be prohibited, unless one of the conditions described in the second paragraph of Section 2 are fulfilled. Moreover, Recital 51 mentions that authentication will require the same precautions as identification.

Based on the above, an IDM system that can process biometric data needs to go through a DPIA because of the nature of the processing that identity management systems demand. In this context, biometric data is always used to uniquely identify a natural person, which is the type of processing that Article 9 refers to. Additionally, Article 35(3.b) states that the processing of such data on a large scale requires a DPIA. Recital 91 underlines the necessity of a DPIA if the scope of processing is for making decisions or profiling regarding specific natural persons. Consequently, this involves the processing of biometric data, and generally, it can be viewed as a field of landmines where an IDM system can easily fulfill several criteria that trigger the need for a data protection impact assessment. Finally, since the data subjects have the right to withdraw their consent (for processing or storing their information) at any time it is crucial to keep track of the biometric data throughout the life-cycle of the operations. For that reason a DPIA is very useful not only for being compliant, but also for having the ability to demonstrate compliance.

3 Related work

Meints et al. [Me08] outlined some of the key data protection principles concerning biometrics based on Article 29 Working Party's paper on biometrics [Ar03] and the Directive 95/46/EC. The GDPR repealed the latter, but the principles were kept and can be found throughout the Articles of the GDPR. Additionally, Meints et al. [Me08] pointed out relevant privacy-related risks regarding biometric data: identity theft, extraction and use of additional information in biometric reference data, linking of biometric data with other personal data and profiling, tracking and surveillance using biometric systems, misleading expectations of the reliability of biometric systems and violation of the right to informational self-determination by forcing people to use biometric systems. In [Re05] Rejman-Greene formulated 8 principles based on the Directive 95/46/EC. Some of these points can also

be found in [Me08], but in addition it mentions an important principle: *"Not keeping the data for longer than its necessary for the stated purposes (that is in a form that permits identification of the data subjects)"*.

Wuyts et al. [WJ15] evaluated the LINDDUN methodology using two case studies and concluded that it is easy to learn and useful in practice, but its completeness needs to be improved. In a study conducted by Veseli et al. [Ve19] LINDDUN was used for privacy risk assessment against a cloud-based platform named Identity Wallet Platform. In a previous work [BG19], we compared LINDDUN, ISO/IEC 29134:2017, and the framework from the Commission Nationale de l'Informatique et des Libertés (CNIL) which is an independent French administrative regulatory body. We evaluated their performance based on principles of data protection and privacy impact assessment collected from an extensive literature review. Hansen et al. [HJR15] identified six privacy protection goals for identity, and in another work [Ha13] the authors outlined some of the major privacy risk factors threatening these goals. In this paper, we use the identified risks as benchmarks along with the privacy risks of Meints [Me08] (that focus on biometrics), and other points identified in the literature to see how well are addressed by the frameworks we selected for our case study.

4 Privacy Protection Goals and Risks

The analysis in this paper focuses on privacy risks that occur when personal information is mishandled, and consequently, an individual's privacy is threatened. In our case study, the emphasis is given on finding privacy risks related to IAM [Ha13, Pa12] and raw biometric information or templates created from them. Privacy risks are divided into two tables based on if they are generally related to IAM or specifically to biometrics. The points discussed below are related to IAM and are collected in Table 1. IAM uses tokens to assign roles for access control. These are technical artifacts providing assurance about identities.

Token frequency and duration of use: information transfer between identity providers and service providers can allow profiling when the same token is used repeatedly. An identity management system should be designed in a way that prevents the activities of the end-user to be linked. For example, several services rely on Google and Facebook as an identity provider.

Token use and purpose: if a token is used for multiple purposes or services, it might be abused or processed illegally. It is essential to define who uses the ID infrastructure and determine how probable it is for the service providers to link different identifiers of the same user.

Provisioning: a token must be monitored through its whole life-cycle. Creation of a token should incorporate principles like data minimisation and clear purpose of use. Updating tokens should be possible for ensuring its authenticity and integrity. In addition, other attributes like deletion, transmission, and consent management should be available for the user.

Secrecy: a token needs to be classified according to the necessary secrecy level, such as inferable, public, or obfuscated supports token secrecy against linkability, re-identification, and unauthorised use. Inferable tokens are easily guessed, whereas public tokens are known by multiple people in an organisation or are available on several databases. In contrast, obfuscated tokens need to remain secret like a credit card pin.

Claim Type: attaching a claim to the token can increase its security. There are three types of claims: 1: information like a password, 2: physical characteristics like a fingerprint, 3: physical items like a card, or a USB key. Combining secrets with high entropy raises the cost for an attacker. Security levels can be managed based on single or multiple-factor authentication.

Obligation and Policy: a privacy policy for checking and evaluating data protection operations should be present.

Assignment and Relationship: defining how a token is created, assigned, and knowing who controls the token can contribute to reducing privacy or security risks. A token can be chosen by a person, can be jointly established, or forced upon by an authority.

Mobility: the following four properties characterize the degree of mobility of a token: *copyable*: how easily it can be copied; *remotely usable*: if it can be used for remote identity management; *concurrently usable*: if it can be used in parallel sessions; *immobile*: if it must be physically present to be used.

Value at risk: The significance of token security has to be classified based on the following events: loss, misuse, disclosure, disruption, theft and cost of replacing it.

Biometric systems handle biometric reference patterns that are attached to a person's identity. In risk and impact analysis, each of the above categories contributes to biometric privacy breach consequences. As explained in detail in [Pa12], major risks are introduced from the use of biometric identifiers when used by third parties without a data subject's consent (can lead to involuntary de-anonymization and profiling by others). The loss of biometric tokens (reference patterns) renders a fingerprint or face unusable (in case of primitive biometrics), which damages the data subject's ability to use this biometric feature in the future. Furthermore, the identified privacy risks specifically for biometric use cases [Me08],[Re05] are analysed as well as whether or not different DPIA methods address them. Table 2 presents the aforementioned privacy risks.

5 Case Study

5.1 Introduction to SWAN

The SWAN project (Secured access over Wide Area Network) is funded by the Research Council of Norway with the goal of researching and developing measures and innovative

technologies that lead to a usable, economic, and privacy-preserving access control based on biometric authentication. The project harvested and processed the following biometric characteristics: face, iris, fingers, and voice. Additionally, name, age, gender, and email address were collected from the data subjects. Data were collected for research purposes and specifically for developing a privacy-preserving access control platform based on biometrics. The envisioned application of the project is to authenticate banking transactions and to secure access to services over broadband and mobile networks. The project overcomes the need for centralized storage of biometric data by storing biometric references locally, and authentication is done based on a pre-shared secret. The inner workings of the authentication protocols were published in [HB10] and [SRB18].

5.2 Methodology

The SWAN project was first assessed using the CNIL's framework, followed by the ISO/IEC standard 29134:2017. Only after the impact assessments were conducted, we performed the analysis comparing its results to the specific privacy risks related to IDM and biometrics. This was done for avoiding being influenced during the assessment and not look for specifically these questions (or learn them after the first assessment), but to see if they can be discovered with the help of the frameworks. For each privacy risk, we analysed if performing the steps of a DPIA helps to identify the risk. If the framework addresses it, the point receives a checkmark ✓. The bias introduced by knowing the project is inevitable since it is a prerequisite for performing the DPIA. Note that neither of these is an exhaustive list, but they are meant to test the DPIA frameworks in a structured manner. The first table contains points for general IAM, whereas the second table focuses on questions specifically about biometrics.

Privacy Protection Risks in general IAM	ISO	CNIL
Token frequency and duration of use	-	-
Token use and purpose	✓	✓
Provisioning	✓	✓
Secrecy	-	-
Claim Type	-	✓
Obligation and Policy	✓	✓
Assignment and Relationship	-	-
Mobility	✓	-
Value at Risk	✓	✓

Tab. 1: Privacy Risks in IAM

The frameworks are performing equally in IAM related topics. Five out of nine points are addressed for each, but even jointly, they don't cover every important aspect.

Privacy Protection Risks in Biometrics	ISO	CNIL
Identity theft	-	✓
Extraction and use of additional information in biometric reference data	✓	✓
Tracking using biometric systems	-	-
Avoid misleading expectations of the reliability of biometric systems	✓	✓
Violation of the right to informational self determination by not giving other option but to use biometrics	-	✓
Explicit raw data disposal policy	-	-
De-anonymization by third parties	-	-

Tab. 2: Privacy Risk in Biometrics

CNIL performs better on addressing biometric specific privacy protection goals, but still, several questions are not addressed by either of the frameworks. This shows that general DPIA methodologies have to be complemented with additional sector-specific supporting materials.

6 Summary

In this paper, we have introduced privacy and data protection with a focus on biometric identification. We discussed the regulatory background and the existing principles for risk and impact assessment of biometric identity management with respect to privacy, as well as related privacy protection goals. In a direct comparison of the ISO/IEC 29134:2015 standard with the CNIL methodology, we found the CNIL method to be slightly better prepared for impact analysis of biometric systems. In general, IAM related questions performed equally, whereas in privacy protection risks for biometrics CNIL covered four out of seven points. In contrast, ISO addresses only two. However, none of these methods can be considered being a standalone solution for applications related to biometrics. The danger of de-anonymization by third parties is a critical privacy issue that is not addressed at all. The fact that CNIL performed better in this comparison regardless of the ISO standard better overall process shows that a good workflow provides no guarantee for addressing specific technological or sector-specific questions. For this reason, we emphasize the importance of developing official supporting documents and guidelines elaborating on privacy and data protection principles related to this rapidly growing field.

References

[Ar03] Article 29 Data Protection Working Party: WP 80 – Working Paper on Biometrics. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf, retrieved on 20.02.2020.

[Ar17] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, retrieved on 08.08.2019.

[BG19] Bisztray, Tamas; Gruschka, Nils: Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In: Nordic Conference on Secure IT Systems. Springer, 2019.

[Ca13] Campisi, Patrizio: Security and privacy in biometrics. Springer, 2013.

[Eu11] Privacy and Data Protection Impact Assessment Framework for RFID Applications. https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications, retrieved on 08.08.2019.

[Eu16] European Parliament & Council: Regulation (EU) 2016/679 – Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119(4.5.2016):1–88, April 2016.

[Ha13] Hansen, Marit et al.: FutureID Deliverable D22.3 Privacy Requirements. Technical report, 2013.

[HB10] Hartung, Daniel; Busch, Christoph: Biometric Transaction Authentication Protocol. In: 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies. pp. 207–215, July 2010. ISSN: 2162-2116.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops. pp. 159–166, 2015.

[Me08] Meints, Martin et al.: Biometric Systems and Data Protection Legislation in Germany. In: 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp. 1088–1093, 2008.

[Pa12] Paintsil, Ebenezer: Evaluation of privacy and security risks analysis construct for identity management systems. IEEE Systems Journal, 7(2):189–198, 2012.

[Re05] Rejman-Greene, Marek: Privacy Issues in the Application of Biometrics: a European Perspective. In (Wayman, James; Jain, Anil; Maltoni, Davide; Maio, Dario, eds): Biometric Systems: Technology, Design and Performance Evaluation, pp. 335–359. Springer London, London, 2005.

[Sm09] Smart Grids Task Force. https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force, retrieved 20.02.2020.

[SRB18] Stokkenes, Martin; Ramachandra, Raghavendra; Busch, Christoph: Biometric Transaction Authentication using Smartphones. In: 2018 International Conference of the Biometrics Special Interest Group (BIOSIG). pp. 1–5, September 2018.

[Ve19] Veseli, Fatbardh; Olvera, Jetzabel Serna; Pulls, Tobias; Rannenberg, Kai: Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing - SAC '19. ACM Press, Limassol, Cyprus, pp. 1475–1483, 2019.

[WJ15] Wuyts, Kim; Joosen, Wouter: LINDDUN privacy threat modeling: a tutorial. CW Reports, 2015.