Analysis of information security measures embedded in the GDPR

Jan Willemson *Cybernetica*
Tartu, Estonia
jan.willemson@cyber.ee
ORCID: 0000-0002-6290-2099

***Abstract*—This paper takes a viewpoint of the information security officer whose task is to ensure the optimal level of privacy protection for personal information that the organisation processes. We analyse the requirements of the EU's General Data Protection Regulation (GDPR) with the aim of finding out whether all the main aspects of information security management process (prevention, detection, response and recovery) are covered in a well-balanced manner. Our main finding is that recovery is under-emphasised in the GDPR compared to the other aspects.**

I. Introduction

There is no single definition of information security, but there are three aspects that often emerge [1]:

- **confidentiality** – information has not been disclosed in an unauthorized manner;
- **integrity** – information has not been modified in an unauthorized manner;
- **availability** – access to information is not blocked in an unauthorized manner.

Privacy is an even more loosely defined notion understood differently by different authors [2], [3], [4], [5]. From the information security perspective, privacy is closely related to confidentiality, and these terms are sometimes even used interchangeably. In this paper, however, we will clearly distinguish the two. For our treatment, confidentiality is a *property* ensured by the *data management processes*, but privacy is rather an *expectation* of the *data subject*.

In the era of networked data storage and processing, it is however unreasonable to assume that the data subject alone is capable of fulfilling this expectation. This is where privacy legislation such as EU's General Data Protection Regulation (GDPR) comes to help.

Perhaps it is easier to grasp the essence of privacy through it complement – privacy loss. It should not be understood merely as some data labelled "confidential" becoming public. In our treatment, we require that an actual *loss* occurs as a result. This loss may, but does not have to be directly monetary. We also consider e.g. reputation damage or community stigmatization as potential losses. Thus, we understand privacy as a state of the data subject where such harm has not occurred. Stating it otherwise, we are only concerned with privacy, because there is potential harm that may occur as a result of unintentional actions or deliberate attacks.

This paper has been supported by the Estonian Research Council under the grant number PRG920.

In order to protect any physical or digital asset, the asset manager can apply a number of *security measures*. These can, in general, be divided into four categories [6].

- **Prevention** These are the measures designed to ensure that the harm does not occur in the first place. Typical measures in this category include locks and steel doors in the physical domain, or firewalls and access control in the case of information protection.
- **Detection** It is not always possible or economically reasonable to prevent all the potential losses. Some harm may be accepted as a residual risk, but in this case it is essential to detect such a situation as soon as possible in order to limit the loss. In the physical domain we consider e.g. surveillance cameras belonging to this category, whereas in the case of information systems we may encounter log monitoring and intrusion detection systems.
- **Response** Once a harmful event (such as privacy breach) is detected, it has to be reacted upon. In the physical world we call the police, whereas in the digital domain we may contact a Computer Emergency Response Team (CERT).
- **Recovery** Even despite all the preventive and reactive efforts, the loss may still happen. In this case it is crucial to also foresee mechanisms for disaster recovery. Both in the physical and digital world we may have e.g. insurance to help us restore the situation as it was before the damage.

We can not really say that one of these categories is more important than another. Each system (be it physical or digital) must find an equilibrium here. In this paper, we will take a look at the information security mechanisms as stated by the GDPR, identify their measure categories, and assess the balance between them.

The paper is organised as follows. We first review some previous work in Section II. Then Section III present sour analysis of the relevant articles of the GDPR, followed by the analysis on Section IV. Finally, Section V draws some conclusions and sets directions for future work.

II. Related work

The declarative nature of GDPR has motivated several lines of research aiming at bringing more operational aspects into

the picture.

Tom *et al.* created a formal model of entities and their relationships as stated in the GDPR. In addition, they also created a model of the rights granted by the GDPR, mapping these to the identified entities [7]. Based on these models, Matulevičius *et al.* later proposed an approach for managing GDPR compliance in business processes [8].

Ayala-Rivera and Pasquale take the viewpoint of an organisation that needs to assess GRPR compliance of their operations. They propose GuideMe, a 6-step systematic approach that supports elicitation of solution requirements that link GDPR data protection obligations with the privacy controls that fulfil these obligations and that should be implemented in an organization's software system [9].

As the GDPR is rather an involved regulation, its practical implementation is challenging without dedicated tools. This is why a number of working groups have proposed and developed respective solutions [10], [11], [12], [13], [14].

Besides general guidelines and applications for GDPR compliance, this domain has also been studied in some specific contexts like big data [15] and continuous integration [16].

III. Security measures as defined and mandated by the GDPR

GDPR comprises of 99 articles organised into 11 chapters, accompanied by 173 recitals elaborating further on the topics covered by the main articles[1].

Even though the primary target of the GDPR is privacy protection of the data subjects, it covers much of the general privacy ecosystem, including for example data transfer between different jurisdictions, cooperation between the authorities and certification. A significant part of the regulation is not concerned with security measures at all, but rather lists the ground definitions, states requirements to organisational setup and involved processes, presents relations to the other regulations, etc.

In the current paper, we have concentrated more specifically on the viewpoint of the data subject. During the course of this research, we went through all the 99 articles, assessing each one in regards to whether it has *direct* security-related effect on the subject. As a result, we identified 23 articles.

As the next step, we categorised the measures stated in the respective articles as *prevention*, *detection*, *response* or *recovery* mechanisms. Of course, such a categorisation is, to an extent, subjective, and can be debated. In order to support the potential debate, we have also added a short rationale together with every assessment.

Of course, these assessments are subjective and can be debated. Hence, the resulting analysis should be condider as an opinion, rather than a conclusive irrefutable statement.

Informing the data subject about the processing This measure is covered in various settings by GDPR Articles 12-15. For example Article 13 mandates informing the data subject in case the data to be processed is obtained directly from the subject him/herself. Article 14, on the other hand, puts a similar requirement on the data controller even in the case the data about the subject has been obtained from somewhere else. One way or another, from the data subject's point of view, these measures can be classified as *detecting* the act of data processing (and hence the potential for privacy leakage).

Right to erasure ('right to be forgotten') Article 17 of GDPR ensures the data subject's right to require from the "*controller the erasure of personal data concerning him or her*". This is targeted towards disabling future potential misuses of the personal data, and hence we classify it as a *prevention* measure.

Right to restriction of processing Article 18 of GDPR grants the data subject "*the right to obtain from the controller restriction of processing*" under several scenarios, e.g. when the controller no longer needs the personal data, or when lawfulness of the processing has been contested. Similar to the effect of Article 17, this measure is also targeted towards minimizing the threats by limiting the processing, hence we classify it as a *prevention* measure as well.

Right to object In certain scenarios (e.g. direct marketing), the data subject has the right to object data processing under Article 21 even if this processing is happening on the lawful grounds. Similar to the two previous sections, this is also a measure *preventing* the potential privacy breaches.

Data protection by design and by default Article 25 mandates that the controller shall "*implement appropriate technical and organisational measures, such as pseudonymisation [and] minimisation [- - -] in order to meet the requirements of this Regulation and protect the rights of data subjects.*" Furthermore, "*The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.*" This is again a measure designed to *prevent* (or at least limit) the potential privacy breach by limiting the amount of data to be processed to a minimum.

Records of processing activities According to Article 30, "*Each controller [- - -] shall maintain a record of processing activities under its responsibility.*" Such records are useful in the *response* phase in order to find out which party is responsible for a privacy breach, and to estimate the extent of the breach.

Security of processing Despite the very relevant title, Article 32 does not really say much about the actual security measures "*to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*". Rather, it states the necessity to perform risk assessment, and select the measures accordingly. The text of the Article makes references to pseudonymisation and encryption, but these are just examples on par with actions like system testing and making sure data availability can be restored in case of an incident. Thus, we do not assign a measure category to this Article at all.

Informing about the personal data breach Articles 33 and 34 obligate the controller to inform the authorities and the data subject about the personal data breach once it has happened. According to our interpretation, this is a *response* mechanism.

[1] https://gdpr-info.eu/

Data protection impact assessment If there is a "*a high risk to the rights and freedoms of natural persons*", Article 35 mandates that the controller "*shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*". As such, we classify this as a *preventive* measure.

Data protection officer Articles 37-39 foresee the position and responsibilities of a data protection officer in the organisation that processes personal data. The exact effect of this position depends on the implementation details, but in principle, this role can contribute to *prevention*, *detection* and *response* in case of a privacy breach.

Codes of conduct Article 40 encourages drawing up codes of conducts targeted towards formalising the processes of data processing, but also exercising the rights of the data subjects, and notifications of personal data breaches. As such, we classify this measure as contributing to *prevention* and *detection*.

Certification Article 42 encourages "*the establishment of data protection certification mechanisms*". However, these mechanisms contribute no new measures, but rather only certify the already existing ones. Thus we do not classify certification as a security measure of its own right at all.

Right to lodge complaint, get remedy and representation Articles 77 to 80 state the data subject's rights to lodge complaints against supervisory authority, controller or processor, and have effective legal representation on the matter. As such, we view this as a class of *response* actions.

Right to compensation and liability Article 82 foresees the compensation for a data subject "*who has suffered material or non-material damage*" as a result of a privacy breach. From the data subject's viewpoint, this is the only *recovery* mechanism in the GDPR. Articles 83 and 84 also foresee fines and penalties against the party processing the data in case of misconduct, but these do not benefit the data subject directly, so we do not classify these as measures from the data subject's viewpoint.

TABLE I
SUMMARY OF THE GDPR SECURITY MECHANISMS

Article	Prevention	Detection	Response	Recovery
12		+		
13		+		
14		+		
15		+		
17	+			
18	+			
21	+			
25	+			
30			+	
32				
33			+	
34			+	
35	+			
37	+	+	+	
38	+	+	+	
39	+	+	+	
40	+	+		
42				
77			+	
78			+	
79			+	
80			+	
82				+

IV. ANALYSIS

We summarise our findings in Table I.

As stated in Section I, all the four categories of measures have their own role to play in the security infrastructure, and a good balance between them should be targeted. Looking at Table I we can conclude that the prevention, detection and response mechanisms are indeed relatively well balanced with 9, 8 and 10 articles referring to them, respectively.

The recovery mechanisms, however, are very scarce in GDPR, with only one measure (compensation for damage stated in Article 82) present.

Such a situation can, to an extent, be explained by some general considerations. First, recovery mechanisms are typically the most expensive ones, and damages should preferably be prevented rather than dealt with after the fact. This justifies a relatively larger share of prevention mechanisms foreseen in comparison with recovery. However, the measures starting from detection address the situation where harm (e.g. in the form of data breach) has already occurred. Hence, this kind of reasoning does not help us to understand why recovery mechanisms are underrepresented in comparison with detection and response.

Another possible explanation to this imbalance stems from the nature of data privacy breaches. Once a piece of information leaks, it is often impossible to reverse the effect of this leak – what has become known, can not be unknown. Thus recovery in terms of mandating everyone to forget the leaked information does not really work.

However, this does not mean that other recovery mechanisms besides the right to claim compensation are impossible.

For example, insurance is a universal method to support recovery after the incident. In the context of GDPR Article 82, compulsory data leak insurance could ease the guilty controller or processor to pay the compensation.

Given that the data privacy leaks often result in reputation damage, the measures for reputation restoration can also be foreseen. They do not necessarily have to be financial. Sometimes a public apology is enough, but sometimes restoring someone's reputation assumes wider societal activity. Data processors can be encouraged to take social responsibility fighting e.g. against discrimination based on sexual preferences, health conditions, and other types of oppression based on the information about the individuals.

Another interesting observation about Table I concerns Articles 32 ("Security of processing") and 42 ("Certification"). On one hand, these articles can be expected to contain the main security mechanisms, and the means to assess their correct implementation, respectively. Still, our analysis did not reveal regulations like that. Both of these articles were largely declarative statements that security mechanisms should be deployed and certification should be organised.

Of course, one may argue that GDPR was never meant to

be a security manual. At the same time, as the main part of the current paper shows, a number of security mechanisms are stated across the regulation. What GDPR is missing, in our opinion, is a clear operational standard how to achieve the declared results in privacy protection. As such, it remains halfway, stating some restrictions, but also leaving excessive room for interpretation. As a result, an organisation trying to meet the GDPR requirements may find itself carrying the burden of implementation, but being still unsure if its operations have achieved an optimal level of privacy protection as a result.

To an extent, this problem can be alleviated by the national Data Protection Agencies (DPAs) that can act as information hubs for the local best practices. On the pther hand, they also have to base their privacy protection related decisions and recommendations on the regulations like GDPR. Clear guidelines concerning operational security standards would also make the work of national DPAs considerably easier.

V. Conclusions and future work

This paper took a viewpoint of the information security officer working in an organisation with the aim of establishing the optimal level of privacy protection for personal information that the organisation processes.

The main regulation that such an officer has to take into account in the EU is GDPR. Even though the general idea behind GDPR is good, it can hardly be considered a balanced document. It states a number of desired target properties and restrictions, but it does not clearly list the methods sufficient to achieve these properties.

At the same time, it refers to several components of information security management process, but does not strike a balance between the different aspects of it. Most notably, our analysis showed that the means for recovery after privacy breach incidents are under-stated in the GDPR.

This observation gives some natural directions for future work. Breach recovery mechanisms definitely deserve more significant attention. This attention does not necessarily have to materialise in the form of a GDPR update, but can also be presented in supplementary operational recommendations. Given that operational recommendations are a weak point of GDPR in general, emergence of such a document would benefit the whole ecosystem on a larger scale than just stating some additional recovery mechanisms.

References

[1] D. Gollmann, *Computer Security*. Wiley, 2011, 3rd edition.

[2] R. B. Parker, "A definition of privacy," *Rutgers L. Rev.*, vol. 27, p. 275, 1973.

[3] A. D. Moore, "Defining privacy," *Journal of Social Philosophy*, vol. 39, no. 3, pp. 411–428, 2008.

[4] D. J. Solove, "Understanding privacy," 2008, Harvard University Press, https://ssrn.com/abstract=1127888.

[5] K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams, "A data privacy taxonomy," in *British National Conference on Databases*. Springer, 2009, pp. 42–54.

[6] H. Bidgoli, *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*. John Wiley & Sons, 2006, vol. 3.

[7] J. Tom, E. Sing, and R. Matulevičius, "Conceptual representation of the GDPR: model and application directions," in *Perspectives in Business Informatics Research - 17th International Conference, BIR 2018, Stockholm, Sweden, September 24-26, 2018, Proceedings*, ser. Lecture Notes in Business Information Processing, J. Zdravkovic, J. Grabis, S. Nurcan, and J. Stirna, Eds., vol. 330. Springer, 2018, pp. 18–28.

[8] R. Matulevičius, J. Tom, K. Kala, and E. Sing, "A Method for Managing GDPR Compliance in Business Processes," in *Advanced Information Systems Engineering - CAiSE Forum 2020, Grenoble, France, June 8-12, 2020, Proceedings*, ser. Lecture Notes in Business Information Processing, N. Herbaut and M. L. Rosa, Eds., vol. 386. Springer, 2020, pp. 100–112.

[9] V. Ayala-Rivera and L. Pasquale, "The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements," in *26th IEEE International Requirements Engineering Conference, RE 2018, Banff, AB, Canada, August 20-24, 2018*, G. Ruhe, W. Maalej, and D. Amyot, Eds. IEEE Computer Society, 2018, pp. 136–146.

[10] Y. S. Martín and A. Kung, "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering," in *2018 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2018, London, United Kingdom, April 23-27, 2018*. IEEE, 2018, pp. 108–111.

[11] P. Ryan, M. Crane, and R. Brennan, "GDPR Compliance Tools: Best Practice from RegTech," in *Enterprise Information Systems - 22nd International Conference, ICEIS 2020, Virtual Event, May 5-7, 2020, Revised Selected Papers*, ser. Lecture Notes in Business Information Processing, J. Filipe, M. Smialek, A. Brodsky, and S. Hammoudi, Eds., vol. 417. Springer, 2020, pp. 905–929.

[12] A. Tsohou, E. Magkos, H. Mouratidis, G. Chrysoloras, L. Piras, M. Pavlidis, J. Debussche, M. Rotoloni, and B. G. Crespo, "Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 531–553, 2020.

[13] L. Piras, M. G. Al-Obeidallah, A. Praitano, A. Tsohou, H. Mouratidis, B. G. Crespo, J. B. Bernard, M. Fiorani, E. Magkos, A. C. Sanz, M. Pavlidis, R. D'Addario, and G. G. Zorzino, "DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance," in *Trust, Privacy and Security in Digital Business - 16th International Conference, TrustBus 2019, Linz, Austria, August 26-29, 2019, Proceedings*, ser. Lecture Notes in Computer Science, S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa, and I. Khalil, Eds., vol. 11711. Springer, 2019, pp. 78–93.

[14] D. Alkubaisy, L. Piras, M. G. Al-Obeidallah, K. Cox, and H. Mouratidis, "ConfIs: A Tool for Privacy and Security Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design," in *Proceedings of the 16th International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE 2021, Online Streaming, April 26-27, 2021*, R. Ali, H. Kaindl, and L. A. Maciaszek, Eds. SCITEPRESS, 2021, pp. 80–91.

[15] M. Rhahla, S. Allegue, and T. Abdellatif, "Guidelines for GDPR compliance in Big Data systems," *J. Inf. Secur. Appl.*, vol. 61, p. 102896, 2021.

[16] Z. S. Li, C. M. Werner, N. A. Ernst, and D. E. Damian, "GDPR Compliance in the Context of Continuous Integration," *CoRR*, vol. abs/2002.06830, 2020. [Online]. Available: https://arxiv.org/abs/2002.06830