The Structure of Data Privacy Compliance

Alexandra Klymenko, Stephen Meisenbacher and Florian Matthes

Technical University of Munich, School of Computation, Information and Technology, Department of Computer Science, Boltzmannstr. 3, Garching, 85748, Germany

Abstract

Achieving Data Privacy Compliance involves a dynamic process requiring the expertise of many roles, particularly legal and technical experts, and it ultimately revolves around the goal of data protection, particularly in technical systems. While this goal may be clear, the inner workings and overall structure of the compliance process remain under-researched. In particular, the roles involved in the process of data privacy compliance and the nature of the interactions between them have not yet been investigated or formalized in a structured manner. In this work, we present such a structure, based on a series of interviews conducted with privacy professionals with varying responsibilities in compliance programs.

Keywords

Data privacy, privacy compliance, organizational structure

1. Introduction

With the growth in scrutiny placed upon data processing entities, particularly in light of recent regulations such as the General Data Protection Regulation (GDPR), the importance of proper privacy compliance programs has concurrently risen. Essentially, the demonstration of compliance with regulations involves the safeguarding of personal information via organizational and technical measures. In order for such measures to be successfully implemented, a series of (inter)actions and decisions must be carried out. Therefore, compliance is not an isolated action, but rather a *process*, in which multiple roles and responsibilities are involved.

In the changing landscape of data protection in response to rapidly advancing technologies and the regulatory response thereto, the process of privacy compliance has been continuously evolving. As such, little work has been performed to achieve a better understanding of such processes from an organizational perspective. This includes the different roles involved, their general categorization, the interactions between these roles, as well as the nature of such interactions.

This work presents the results of our initial investigation into structuring the process of privacy compliance with a focus on the implementation of *technical* measures [1]. In particular, we introduce the primary roles involved, whose responsibilities are crucial to the success of compliance programs, or the processes put into place to achieve compliance. These insights are obtained from a series of interviews with privacy professionals working in these processes. Next, we discuss the interactions taking place between these roles. Finally, as an additional new contribution to this extended abstract, we visualize our findings in a compliance structure, which we pose to be a representation of the general makeup of privacy compliance programs.

The structure of our work is as follows. Section 2 introduces the foundations of our work, upon which we built. Section 3 outlines our research design, the results of which are presented in

CEUR-WS.org/Vol-3512/extendedabstract1.pdf

CIISR 2023: 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research, co-located with the 18th International Conference on Wirtschaftsinformatik (WI 2023), September 18, 2023, Paderborn, Germany

alexandra.klymenko@tum.de (A. Klymenko); stephen.meisenbacher@tum.de (S. Meisenbacher); matthes@tum.de (F. Matthes)

0000-0001-7485-2933 (A. Klymenko); 0000-0001-9230-5001 (S. Meisenbacher); 0000-0002-6667-5452 (F. Matthes)

© 2023 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

Section 4, which culminates in our Privacy Compliance Structure (PCS). We conclude our work in Section 5, describing points of future work.

2. Background and Related Work

Modern privacy regulations, such as the GDPR or CCPA, establish guidelines for the responsible handling of personal data and require strict compliance, i.e., "ensuring adherence of an organization, process or (software) product to laws, guidelines, specifications and regulations" [2]. More specifically, the process of privacy compliance involves implementing various technical and organizational measures to ensure the protection of personal data, and, as such, it requires the expertise and involvement of specialists of various professional backgrounds. Research in the field of regulatory compliance of software systems, such as by Maxwell et al. [3], has demonstrated that software engineers cannot independently reason about compliance requirements. Likewise, Altman et al. [4] promote a hybrid legal-technical approach to privacy protection, arguing that without legal input, the technical solutions developers create to achieve regulatory compliance may prove ineffective in delivering strong privacy protection and risk non-compliance with regulations. Usman et al. [5] also point out the need to coordinate and align different compliance activities and roles, highlighting some of the difficulties that occur in the process. In this regard, Klymenko et al. [6] describe eight concrete challenges in the technical-legal interactions that occur in the process of data privacy compliance. In the following extended abstract, we aim to structure the roles and interactions involved in this process, in order to support further research on addressing current issues and advancing the overall efficacy of privacy compliance.

3. Methodology

We perform qualitative research following Grounded Theory methodology as described by Hoda et al. [7] by conducting semi-structured interviews with privacy experts in legal and technical sectors. To initiate the study, we developed an interview guide consisting of a pre-defined set of questions that were sent to participants in advance. These questions were designed to gain insights into the various roles, responsibilities, and interactions involved in the implementation of privacy requirements. We recorded and transcribed each interview, subsequently analyzing the data through coding and constant comparison, guided by thematic analysis [8]. This process continued until sufficient information was collected, allowing us to conclude the study. In particular, the main stopping criterion was the observation of a saturation of themes in our thematic analysis. In total, 9 legal experts and 7 technical experts were interviewed. Table 1 provides further information on the interviewees, where participant ID suffixed with a 'T' denotes a technical expert, 'L' a legal, and 'LT' a technical/legal expert. *Exp*. denotes years of experience (parentheses indicate experience specifically in privacy), and *Dur.* the duration of the interview in minutes. The interviews lasted for approximately an hour and were conducted via Zoom.

4. The Privacy Compliance Structure

4.1. Roles

Through the interview study, three overarching categories of roles were highlighted, each of which participates in the privacy compliance process from a different angle. In the interview discussion, the goal was not only to learn about the role of the interviewee, but also about relevant interactions with other roles, including the responsibilities of these further roles. Following the interviews, these roles and their responsibilities were extracted, and they are outlined below.

Table 1
Interview study participants

ID	Position	Organization	Exp.	Dur.
I1-T	Privacy Engineer	Large US media conglomerate	10+ (1)	54
I2-2	Privacy/Security Architect	Large German multinational software corporation	6	52
I3-L	Privacy and cybersecurity lawyer	US law firm	20+	32
I4-T	Privacy Engineer	Large US multinational tech company	5+ (4)	70
I5-LT	DPO, Managing Director	Small German data protection software company	4	50
I6-T	Software Architect	Large German multinational tech conglomerate	3	50
I7-L	Lawyer/external DPO	Small German data privacy company	20+	55
I8-L	Group Data Protection Counsel	International financial technology corporation	6	60
I9-T	Privacy Engineer	Large US Tech Corporation	8	65
I10-LT	Legal Counsel	Global Web Consortium	25	60
I11-L	Legal Counsel	German-based digital privacy consulting firm	3	50
I12-L	DPO	German-based consulting firm	20 (3)	55
I13-T	Security and Privacy Architect	Large German multinational tech conglomerate	3	60
I14-L	Compliance Officer	British-based news corporation	3	50
I15-T	Privacy Engineer	Chinese multinational tech corporation	15	60
I16-L	Legal Associate	Indian-based law firm	3	55

4.1.1. Legal

The first major role category consists of *legal experts*, which generally refer to practicing lawyers or legal associates, often specialized in data privacy or cybersecurity. These roles can be filled internally, or contracted to external legal counsel. The responsibility of these roles is to provide legal support and advice regarding the legal requirements set forth by relevant laws and regulations for privacy compliance.

Another type of legal role comes with the *consultant*. In the absence of or in supplement to lawyers, consultants are important to providing expert knowledge of the proper handling of data, also in light of relevant legal requirements. While consultants often may be a key point of the compliance process, these roles are often not practicing lawyers, showing that legal expertise may come in multiple forms.

A third type of legal role, although not explicitly legal, is that of the *compliance team*. Headed by a *Compliance Officer*, the compliance team is responsible for spearheading compliance activities, including assessing operational risk and ensuring that compliance steps are properly in line with data privacy principles. While the presence of such teams can be observed in practice, it is not clear how widespread such a unit is.

4.1.2. Technical

The process of privacy compliance also requires the involvement of technical experts, especially for the translation of legal requirements into technical solutions. As such, various technical roles were revealed to be involved, which we categorize under the term of *Development*. The first of these is the *product team*. Led by the *Product Owner*, the team is responsible for identifying and assessing potential privacy risks in a proposed product or project. Particularly with the Product Owner, this role becomes the "first point of contact" for ensuring privacy in a specific system.

Also important to the technical side of privacy compliance is the general role of *architects*. *Software Architects* are responsible for the design, rather than implementation, of systems, and it is in this phase where privacy matters must be first addressed. Architects may sometimes be specialized as *Privacy (and Security) Architects*, and also *Enterprise Architects* in larger organizations. In these roles, the design of privacy-preserving systems is crucial in the larger context of privacy compliance.

The role of experts in the *Development* category has been studied in the literature [9][10], speaking to the importance of such roles on the implementation level of privacy requirements. However, both works also make note of the challenges regarding both motivation and ability of

technical experts to comply with privacy regulations. Concrete challenges include tensions with legal [9] or a perceived lack of support [10], suggesting starting points for future work.

Further abstracted from the implementation of technical systems is the role of *management*, which is separated from development. Such roles are tasked with the leadership and direction with regards to compliance programs, ultimately giving the green light for compliance programs. A concrete role often mentioned was the *Chief Information Security Officer (CISO).* The literature also points to the newer role of *Chief Privacy Officer (CPO)* [11]. While such roles do not participate in the implementation of technical measures for privacy compliance, they are indirectly involved via their interaction with Architects and members of the product team.

4.1.3. Go-Betweens

As a final group existing between the legal and technical roles, we define the category of *Go-Betweens* consisting of roles of a more hybrid nature. Concretely, we identified two important roles falling under this categorization.

Particularly since the GDPR came into effect, the role of *Data Protection Officer (DPO)* has become central to the compliance process. The DPO is appointed to steer and monitor all privacy compliance activities, such as Data Protection Impact Assessments (DPIA) or awareness-raising programs. DPOs can be internally filled, or also served by external persons such as consultants. At the core of the responsibilities of this person lies the task of liaising between the letter of the law and how this is interpreted in practice for organization-specific data processing activities. With this, it is clear that the DPO serves a hybrid role, with a leaning towards the legal aspects. Nevertheless, the multi-faceted responsibilities of the DPO include having technical knowledge, as noted by Ciclosi and Massacci [12].

The relatively novel, yet rapidly developing role of *Privacy Engineer* is tasked with bridging the legal-technical gap by providing technical expertise. While the discipline of Privacy Engineering is not yet fully mature, the general role involves creating trust by protecting privacy in technical systems and shaping organizational policy to facilitate this. Privacy engineers do not necessarily need to be experts in the specifics of a system; it is their expertise in privacy design principles that provides value to privacy compliance. As noted by Gürses and del Alamo [13], the rise of this role comes with an increasing need to bridge privacy research and practice, particularly in aligning privacy goals with legal policy, thus solidifying the role of a *Go-Between*.

4.1.4. Other Roles

The interviews also revealed other "external" supporting roles. On the regulatory side, supervisory authorities were indicated as important stakeholders. Within an organization, Marketing, HR, and Sales were also mentioned. Finally, the customer was often listed as a stakeholder, as the "true benefactor" of compliance efforts.

4.2. Interactions

Between the three main categories of roles in privacy compliance come many interactions, consisting of the *Technical-Technical*, *Technical-Legal*, and *Legal-Legal* nature. In defining these types of interactions, we utilize our categorization of roles as introduced above. Thus, an interaction is reported if an interviewee mentioned a relationship between roles within the legal or technical role categories, or between the two.

4.2.1. Technical-Technical

Within the technical sphere of an organization, interactions occurring in the process of privacy compliance come in two general forms: vertical and horizontal. Vertical interactions refer to the role of management positions, which pass down decisions regarding data privacy, as well as

provide support in liaison with legal experts. Architects may often interact with managers for matters regarding compliance.

More horizontally, privacy engineers will often interact with other technical roles, such as software engineers, in order to provide guidance and policy for the implementation of compliant systems. It should be noted that interactions also occur within a team, e.g., when privacy engineers of various specializations consult with one another.

4.2.2. Technical-Legal

As the process of privacy compliance is inherently interdisciplinary, technical-legal interactions are commonplace and almost necessary to ensure the success of compliance programs. The interviews highlighted that many of these interactions take place between legal experts such as lawyers and the technical leadership of an organization, i.e., management. In these interactions, the interpretation of legal requirements becomes very important for leaders to make informed decisions regarding privacy.

For other technical roles, not in management positions, the main point of contact regarding legal matters is the DPO. As access to the DPO is much more readily available than to lawyers, the DPO becomes a de facto Go-Between in bridging the technical-legal divide. This type of interaction, initiated by technical roles, can be useful to engineers with legal questions, or, specifically, to validate that legal requirements are being fulfilled in technical implementations.

An interesting question arises whether technical-legal interactions occur in the other direction, where legal roles initiate contact. While this type of interaction was not reported, it can be best observed in the close work of DPOs with Privacy Engineers or in cross-functional teams. Nevertheless, a more in-depth exploration of the legal roles in privacy compliance presents an interesting opportunity for future work.

A final type of technical-legal interaction comes with the existence of *cross-functional* teams. While this is not a common practice, such teams consist of members from different departments, including those that are more technically or legally oriented. These teams serve as an ideal place for cross-disciplinary exchange.

4.2.3. Legal-Legal

While legal-legal interactions were reported, such as those between consultants and lawyers, they are not expounded upon, as this is not the focus of our work.

4.3. The Structure

Based on the insights obtained regarding the roles, responsibilities, and interactions of the privacy compliance process, we propose a structure to illustrate the process and the dynamics within. As such, we have created the Privacy Compliance Structure (PCS), presented in Figure 1.

The PCS was created as follows. Firstly, the descriptions of the roles held by the interviewees were consolidated, serving as the foundation for the structure. Next, the interviews were analyzed for mentions of other roles in privacy compliance; more importantly, the nature of interaction between this newly mentioned role and the role of the interviewee was noted. This helped to form the basis of the interactions seen in Figure 1. Finally, the major sections in the structure, e.g., *Development*, were positioned to facilitate the nature of the interactions, as described above. For example, the vertical interaction between Management and Development is clear, and the close work between Privacy Engineers and DPOs is also reflected.

In Figure 1, solid single-directional arrows represent designated reporting lines, whereas single-directional dashed lines represent indirect reporting lines (where direct interaction is rare). Solid bi-directional arrows denote exchange rather than reporting lines, and hollow bi-directional lines indicate that two roles may be served by the same person. Finally, a cyclical arrow denotes when exchange occurs within a team.

5. Conclusion

In this work, we outline the components that are part of the process of privacy compliance, namely the roles, their responsibilities, and the interactions within. Using these findings, we construct a Privacy Compliance Structure that mirrors the above-mentioned components. In presenting this structure, we hope to provide structure to the dynamic process of privacy compliance, particularly in the implementation of technical measures.

As suggestions for future work, we see that a validation of the proposed structure is necessary to boost the generalizability of the model. To accomplish this, compliance programs of various organizations, from large and small, as well as those in differing domains, should be studied. Targeted case studies may be a useful approach for this. In addition, as the field continues to evolve, the inclusion of novel and currently not considered roles should be emphasized. As such, we hope that our base structure can be refined, updated, and evaluated.

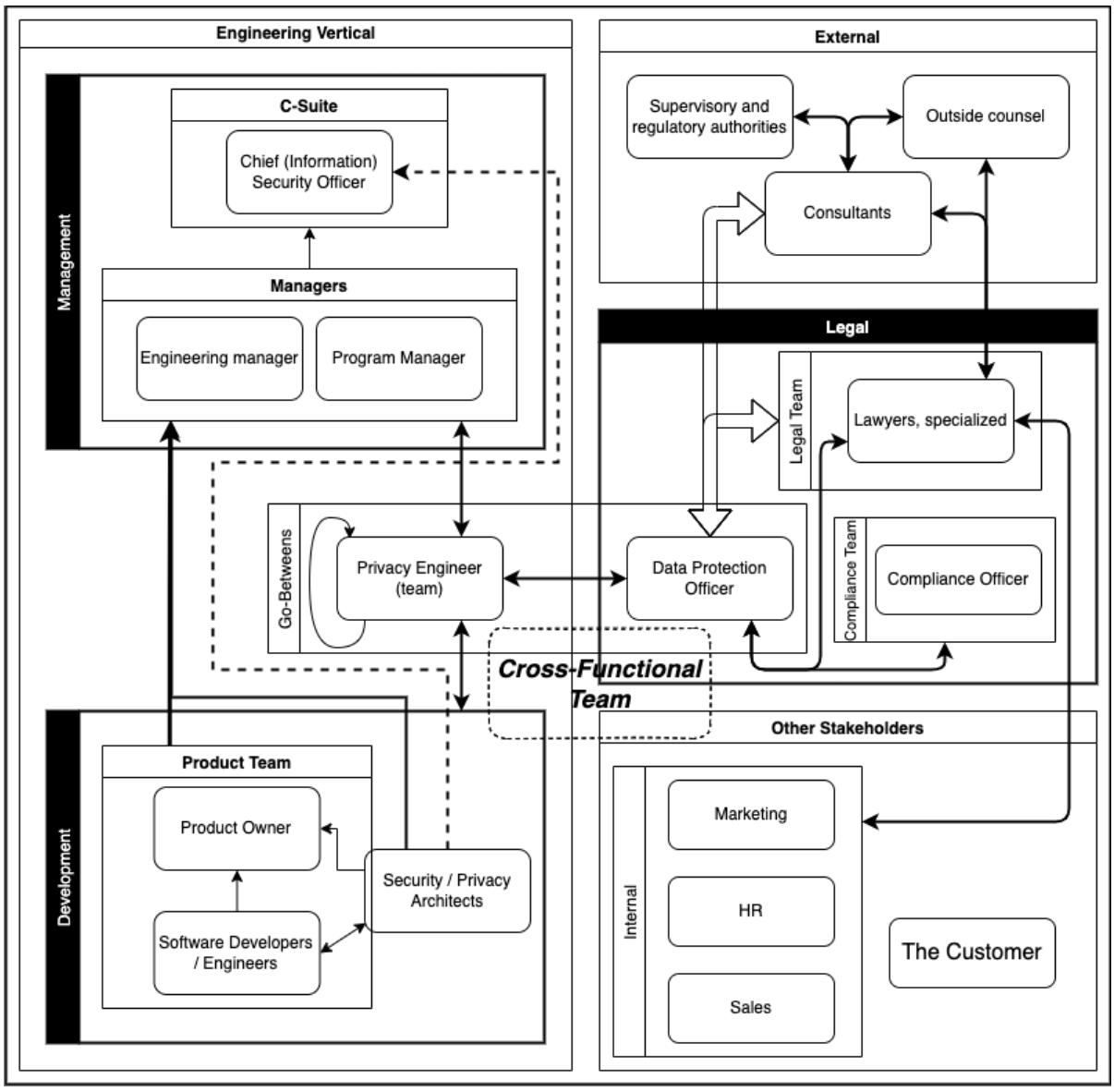

Figure 1: The Privacy Compliance Structure

Acknowledgements

This work has been supported by the German Federal Ministry of Education and Research (BMBF) Software Campus grant LACE 01IS17049.

References

[1] O. Klymenko, O. Kosenkov, S. Meisenbacher, P. Elahidoost, D. Mendez, and F. Matthes, Understanding the Implementation of Technical Measures in the Process of Data Privacy Compliance: A Qualitative Study, in Proceedings of the 16th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, 2022, pp. 261–271.

[2] O. Akhigbe, D. Amyot, and G. Richards, A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance, Requirements Engineering, vol. 24, pp. 459–481, 2019.

[3] J. C. Maxwell, A. I. Antòn, and J. B. Earp, An empirical investigation of software engineers' ability to classify legal cross-references, in 2013 21st IEEE International Requirements Engineering Conference (RE), 2013, pp. 24–31.

[4] M. Altman, A. Cohen, K. Nissim, and A. Wood, What a Hybrid Legal-Technical Analysis Teaches Us About Privacy Regulation: The Case of Singling Out, SSRN Electronic Journal, 2020.

[5] M. Usman, M. Felderer, M. Unterkalmsteiner, E. Klotins, D. Mendez, and E. Alégroth, Compliance requirements in large-scale software development: An industrial case study, in International Conference on Product-Focused Software Process Improvement, 2020, pp. 385–401.

[6] O. Klymenko, S. Meisenbacher, and F. Matthes, Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance, AMCIS 2023 Proceedings. 2, 2023.

[7] R. Hoda, J. Noble, and S. Marshall, Grounded Theory for Geeks, in Proceedings of the 18th Conference on Pattern Languages of Programs, Portland, Oregon, USA, 2011.

[8] V. Braun and V. Clarke, Using thematic analysis in psychology, Qualitative research in psychology, vol. 3, no. 2, pp. 77–101, 2006.

[9] K. Bednar, S. Spiekermann, and M. Langheinrich, Engineering Privacy by Design: Are engineers ready to live up to the challenge?, The Information Society, vol. 35, no. 3, pp. 122–142, 2019.

[10] M. Tahaei, K. Vaniea, and A. Rashid, Embedding Privacy Into Design Through Software Developers: Challenges and Solutions, IEEE Security & Privacy, vol. 21, no. 1, pp. 49–57, 2023.

[11] M. Shawosh, M. Bantan, and F. Belanger, Chief Privacy Officer role and organizational transformation in the digital economy, in ICIS 2022 Proceedings, 2022.

[12] F. Ciclosi and F. Massacci, The Data Protection Officer: A Ubiquitous Role That No One Really Knows, IEEE Security & Privacy, vol. 21, no. 1, pp. 66–77, 2023.

[13] S. Gürses and J. M. del Alamo, Privacy Engineering: Shaping an Emerging Field of Research and Practice, IEEE Security & Privacy, vol. 14, no. 2, pp. 40–46, 2016.