Privacy-Protection Regulations and Frameworks for Organisational Data Sharing

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Seyed Ramin Ghorashi, Tanveer Zia, Michael Bewong, Yinhao Jiang

Industry approaches, such as privacy frameworks, provide essential guidelines and best practices for privacy preservation and risk management, focusing on information, standardisation, and privacy risk identification. These frameworks not only align with privacy regulations but also offer technical advice to help organisations protect personal data effectively. It is important to acknowledge there are many other privacy regulations and privacy frameworks; however, privacy regulations such as the General Data Protection Regulation (GDPR) are mandatory, and organisations have a legal obligation to comply with the laws. Nevertheless, privacy frameworks are voluntary tools available for organisations.

Keywords: privacy regulation ; privacy frameworks ; data sharing ; organisations

1. Introduction

Organisations are increasingly engaging in collaboration with third-party entities such as vendors, suppliers, and business partners to leverage data collection and analysis for improved decision making and operational efficiency [1]. These partnerships allow access to specialised knowledge and resources, facilitating efficient data analytics and cost-effectiveness compared to developing in-house capabilities. Data sharing, a practice vital for knowledge growth and informed decision making, is prevalent across organisations regardless of their resources or technology. It is particularly significant in Internet of Things (IoT) contexts, where data exchange between devices and systems is key to enabling smart, connected environments. While organisations already benefit from using consumer data, further advantages can be gained by sharing data with external entities.

However, despite the benefits associated with sharing data with third-party entities, these organisations pose privacy risks to individuals who use their services. This is because these organisations collect, analyse, and share individuals' data, which often includes personally identifiable information (PII) and sensitive data. Consequently, these data-sharing activities raise privacy concerns, as many organisations exploit data for marketing purposes by delivering targeted advertisements and other content [2].

The personal data exchange between primary organisations and their third-party partners significantly raises the risk of privacy breaches. This issue is supposedly addressed by privacy regulations and industrial privacy frameworks. However, a critical problem lies in the existing privacy regulations, which, while mandating organisations to comply with legal standards and enforce privacy policies, often lack specificity in their guidelines. These regulations typically focus more on legal compliance and general privacy protection rather than providing detailed, technical directives essential for robust data protection.

Consequently, both primary and their third-party collaborators are obligated to lean towards the legal aspects and thus often encounter a lack of agreement between the emphasis on legal compliance outlined in regulations and the lack of technical elements essential for establishing robust data security. This difference can lead to the development of privacy policies that, while legally compliant with the law, may not fully address the complexities of data protection in today's digital world. Another issue can also be the level of data importance in protecting personal data. While all organisations have the responsibility of implementing privacy policy measures to protect and maintain the integrity of personal data, third-party entities collaborating with these organisations may not bear the same level of responsibility.

Industry approaches, such as privacy frameworks, provide essential guidelines and best practices for privacy preservation and risk management, focusing on information, standardisation, and privacy risk identification. These frameworks not only align with privacy regulations but also offer technical advice to help organisations protect personal data effectively. Despite previous studies [3][4][5][6][7] examining major privacy regulations and the need for compliance tools, research on these industrial privacy frameworks, particularly in the context of organisational data sharing, remains limited.

2. Privacy Challenges and Disclosure Risks in Organisational Data Sharing

2.1. Challenges in Organisational Data Sharing

Data sharing is a widely acknowledged practice that enhances organisational efficiency and performance by providing insights into processes and technologies. However, it can present challenges, particularly in relation to privacy concerns [8][9]. The nature of data sharing varies among organisations, depending on their business models, such as B2B, B2C, or C2C, which dictate distinct relationship models and privacy policies [10]. Privacy policies are crucial for organisations as they ensure compliance with privacy regulations and safeguard customer privacy. These policies serve as legal documents, informing individuals about how their personal data are collected, processed, and shared [11][12]. Nevertheless, the implementation of privacy policies can differ between organisations, leading to discrepancies between policy statements and actual practices.

The shift towards cross-organisational data sharing, especially in models like B2B, B2C, and C2C, can enhance organisational performance by exchanging personal data for services or goods [13]. However, there is currently no standardised guidance on disclosing personal data-collection details in privacy policies, resulting in variations between organisations' policies [10]. This lack of standardisation can confuse consumers, who may not fully grasp how their data is managed. Intra-organisational data sharing, as practiced by Meta (the parent company of Facebook, Instagram, and WhatsApp), is valuable when internal systems and customer demographics align [8][14].

Privacy policies play a crucial role in protecting customer privacy, but comprehending these documents can be a challenge due to their often lengthy and complex nature [15][16]. Research conducted in the United States revealed that citizens would need to spend an average of 40 min per day just to read all the privacy policies they encounter [17]. Moreover, privacy policies may be influenced by other privacy regulations from various regions worldwide.

One of the significant difficulties organisations encounter when striving for transparency in their privacy policies is in how they use and disclose personal data. Some organisations adopt a permissive approach, sharing personal data with business partners or affiliates, while others primarily use this data internally, as seen with Meta disclosing user information across its subsidiary platforms like Facebook and Instagram [14].

Ensuring the accuracy of information within privacy policies is vital for maintaining customer trust regarding how organisations handle personal data. For instance, Meta, the parent company of Facebook and Instagram, previously provided false information in 2014 regarding automated profile matching between Facebook and WhatsApp. Subsequently, Meta updated its terms of service, requiring users to agree to the new terms. In 2021, Meta modified its privacy policy to allow the sharing of personal information with its affiliates [18][19]. This highlights the evolving nature of privacy policies and their potential impact on users' data privacy.

Privacy policies serve a critical role in defining an organisation's procedures for processing and disclosing personal data [12]. These procedures, known as privacy practices, are essential commitments made by organisations. However, they are not always consistently followed, often due to factors like data breaches or unauthorised access by malicious actors.

Privacy policies offer numerous advantages beyond merely collecting personal data. They also provide crucial information about partners and affiliates with whom data is shared. One of the key benefits of privacy policies is their ability to inform end users about the specific personal data collected. However, these policies often fall short of providing detailed information about the types of personal information shared with affiliates or third-party organisations.

2.2. Organisational Privacy Disclosure Risks

In today's data-driven world, where organisations rely on exchanging high quantities of data with each other to gain valuable understandings, there are challenges in sharing that data, such as privacy risks of disclosure. Privacy risk refers to the potential threats posed to personal information, which can eventually disclose the information of individuals. In the context of organisational data sharing with third-party entities, the potential privacy disclosure risks could take two forms, such identity disclosure and attribute disclosure.

Identity disclosure [20] refers to the risk of re-identification of individual's identities from shared data. The privacy risk arises when personal data are shared with third-party organisations, revealing combinations of different attributes (QID), allowing the adversaries to recognise the data records by profile-mapping the QID together. The attribute disclosure [21] is achieved by exposing specific QIDs of individuals that were supposed to remain confidential. When data are shared, it might contain sensitive attributes such as medical conditions or financial status.

Two of the main privacy disclosures, identity and attributes, have helped researchers to study many approaches to reduce privacy risks; however, it is important to understand membership disclosure, which could help researchers and regulators to identify privacy risks in organisational data sharing. Membership disclosure [22] occurs when an individual's affiliation to a particular group is revealed without their consent.

3. Organisational Data-Sharing Models

The main value of any organisation is the ability to analyse data based on the information they have. As each organisation has a different type of operation, they could deal with different types of data, and it would suggest what analysis of data they would perform. This analysis is usually conducted on the business side, and the information collected is from their consumers.

A business entity is usually referred to as an organisation that is engaged in commercial, industrial, or professional activities that produce and sell goods or services. The activities of these organisations can define their missions as either for-profit or not-for-profit (non-profit) [23]. There are also organisations that rely on external entities for a specific function or operation. These external entities are called third-party organisations, which are not part of the primary organisation but collaborate together [24]. The consumers, on the other hand, are usually individuals or businesses that purchase and consume the market goods or services of another business [25].

The entities within an organisation are motivated by day-to-day data. These data make up information that is collected from a specific entity, or it is driven data, meaning the data have been populated based on a task or process. There are two types of data that create this different information: first is consumer process data, and the second is business process data.

As discussed above, most organisations fall into a business model category that defines the operation of their business, their business relationships, and their consumers. The main business models are three kinds: B2B, B2C, and C2C.

Business-to-Business, or B2B, is a form of intercompany transaction between two businesses, such that one is a manufacturer or provider and the other becomes a retailer. The transactions between the businesses include trades, purchases, services, resources, and technologies [26][27]. B2B data sharing is normally data about other businesses or consumers that can be used for marketing activities or to make decisions. The data that businesses usually share can be divided into two categories: business process data and consumer process data.

Business-to-Consumer, or B2C, is a relationship between a business and a consumer or business acting as a consumer who are engaged in transactions, such as data, products, and services. The business is usually the entity providing the products and services, and the consumer entity is usually the end user of the goods. Depending on the type of consumer entity, they also provide data to the businesses. These data can be about themselves, or they could be data about how they interact with the products of the businesses [28].

The data that the businesses collect are based on the consumer (business). The businesses take advantage of this collected data to understand their consumers better and determine what their personalities are based on the products and services they provide. There are generally three types of data that businesses are interested in [29]. The personal data of their consumers, the engagement activities of their consumers associated with their business, and the behavioural data of their consumers when it comes to purchasing and using their products and services [29][30]. These data are personal data, engagement, and behavioural data.

Consumer-to-consumer, or C2C, is a business model that allows the transaction of goods and services between two consumers. This model is also known as peer-to-peer (P2P) in the e-commerce business model. This is very similar to the B2C model; however, the consumers are interacting with one another. The C2C platforms are typically electronic market platforms created by businesses to reach more consumers online.

In a C2C platform, the consumers require basic data about one another to communicate. However, the businesses that are facilitating these platforms will collect more data about the consumers' activities. In regard to the process of interaction between the consumers, they may only require the personal information of the consumer. However, the businesses may also collect engagement and behavioural data as part of the process.

Each business model delivers a unique strength based on who the targeted audiences are. In the context of privacy, understanding these business models can help authorities regarding the privacy risks involved. By recognising the type of

audiences and the type of data that businesses are dealing with, organisations can eliminate the possibilities of privacy risks by introducing privacy regulations.

Organisations have a legal obligation to comply with the privacy regulations as they collect, process, and share personal information [31][32]. In this regard, organisations are trying to minimise any potential privacy risk that threatens their business or the privacy of their information by implementing correct privacy practices. Despite the fulfilment of legal obligations, such as complying with privacy regulations and implementing privacy measures, privacy disclosure still occurs. Privacy disclosure is a major disruption for organisations financially and reputation-wise.

A misconception in privacy protections regarding the privacy framework and other measures, such as privacy by design, is the implementation costs and the disruption to the organisation. From an execution perspective, privacy frameworks require planning and a fair amount of consideration in the implementation of the standards. However, compared to privacy by design, the requirement is the implementation of the standards from the foundation level. Simply put, organisations need to re-design their operations for the handling of personal data from a privacy perspective.

3. Privacy-Protection Regulations and Frameworks

3.1. The GDPR in Organisational Data Sharing

In the context of organisational data sharing, the enforcement of privacy regulations in recent years has brought a significant amount of transformation in the data-sharing practices [33]. These legal regulations have been implemented by the governments to protect the privacy of individuals by allowing them to have privacy rights when sharing their information. The most comprehensive privacy regulations, such as the GDPR, have been effective in governance, awareness, and monitoring of the usage of individual data, forcing organisations to protect privacy more proactively [34].

Privacy regulations have introduced a major change in how organisations share data. The requirements for receiving consent prior to data collection, as well as the organisational transparency in data sharing, have encouraged organisations to re-evaluate their data-acquisition and privacy practices, leading to provisioning clear, concise, and easily accessible privacy policies that explain data processing and data sharing [35]. This means organisations must clearly communicate the purposes for which data will be used, which entities will have access to these data, and how these data are protected.

These privacy regulations have also impacted business partners and third-party entities, which also need to show their compliance with the privacy regulations by including appropriate data-protection measures [36]. Any third-party entity that wishes to collaborate with first-party organisations must have due-diligence processes where organisations assess the data-handling processes before sharing any data. For example, if a hospital wishes to share a certain patient's health data with a research institute, the hospital must ensure the research institute complies with the necessary data-protection standards.

3.2. The NIST and Five Safes Privacy Framework

The industrial privacy frameworks have provided guidance for organisations to help them with data privacy and ensure the protection of individuals' personal data. This guidance involves standards, practices, and policies to follow to protect data, but mostly, the guideline's objectives are enhancing the protection level. These scopes are broad, including various approaches such as data collection, processing, storage, and sharing. The guidelines are designed to be applied to a wide range of organisations, such as non-profit organisations, businesses, or governmental organisations.

Privacy frameworks have brought significant change within organisations and other entities, shaping their approach to data privacy and protection techniques, which includes enhancing transparency, increasing individuals' privacy rights, and mitigating privacy risks. One of the significant changes that influenced organisations was the transparency of their data processing with their users, which ultimately forced them to be compliant with privacy regulations. These include guidelines and practices to inform individuals properly and clearly about how their data will be used and shared.

In the last couple of decades, many privacy frameworks have been developed to aid organisations with guidance and practices. One of these privacy frameworks is Five Safes, which was developed to help researchers, particularly in academics. However, with its wide recognition, it is also used in businesses and governmental organisations such as ABS [37]. The main objective of the Five Safes is to create a structured approach for these organisations for better data accessibility and useability whilst minimising privacy risks. The key five dimensions of the framework are (1) people, (2)

projects, (3) settings, (4) data, and (5) outputs. These independent questions are used to conduct a risk assessment scheme for data accessibility and data.

4. Conclusions

In conclusion, the growing trend of organisational collaboration with third-party entities for data acquisition, while enhancing decision-making and operational efficiency, also introduces significant privacy concerns. These external partners often engage in the collection and utilisation of personal and sensitive data, necessitating compliance with government privacy regulations to protect user privacy through robust privacy measures. However, third-party organisations may have varying policies, emphasising the need for comprehensive privacy frameworks that, in conjunction with legal regulations, emphasise standardisation, privacy management, and risk assessment. Such frameworks offer holistic approaches to address the challenges arising in data-sharing partnerships.

References

1. Mariani, M.; Baggio, R.; Fuchs, M.; Höepken, W. Business intelligence and big data in hospitality and tourism: A systematic literature review. Int. J. Contemp. Hosp. Manag. 2018, 30, 3514–3554.
2. Nussbaum, E.; Segal, M. Privacy vulnerabilities of dataset anonymization techniques. arXiv 2019, arXiv:1905.11694.
3. Aljeraisy, A.; Barati, M.; Rana, O.; Perera, C. Privacy laws and privacy by design schemes for the internet of things: A developer's perspective. ACM Comput. Surv. Csur 2021, 54, 1–38.
4. Arellano, A.M.; Dai, W.; Wang, S.; Jiang, X.; Ohno-Machado, L. Privacy policy and technology in biomedical data science. Annu. Rev. Biomed. Data Sci. 2018, 1, 115–129.
5. Koops, B.-J.; Leenes, R. Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. Int. Rev. Law Comput. Technol. 2014, 28, 159–171.
6. Okoyomon, E.; Samarin, N.; Wijesekera, P.; Elazari Bar On, A.; Vallina-Rodriguez, N.; Reyes, I.; Feal, Á.; Egelman, S. On the ridiculousness of notice and consent: Contradictions in app privacy policies. In Proceedings of the Workshop on Technology and Consumer Protection (ConPro 2019), in Conjunction with the 39th IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–22 May 2019.
7. Zhao, K.; Zhan, X.; Yu, L.; Zhou, S.; Zhou, H.; Luo, X.; Wang, H.; Liu, Y. Demystifying Privacy Policy of Third-Party Libraries in Mobile Apps. In Proceedings of the 2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE), Melbourne, Australia, 14–20 May 2023; pp. 1583–1595.
8. Yang, T.-M.; Maxwell, T.A. Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. Gov. Inf. Q. 2011, 28, 164–175.
9. Pearson, S. Privacy Management in Global Organisations. In Communications and Multimedia Security, Proceedings of the IFIP International Conference on Communications and Multimedia Security, Canterbury, UK, 3–5 September 2012; De Decker, B., Chadwick, D.W., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 217–237.
10. Chua, H.N.; Herbland, A.; Wong, S.F.; Chang, Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telemat. Inform. 2017, 34, 157–170.
11. Morton, A.; Sasse, M.A. Privacy is a process, not a PET: A theory for effective privacy practice. In Proceedings of the 2012 New Security Paradigms Workshop, Bertinoro, Italy, 18–21 September 2012; pp. 87–104.
12. Bargh, M.S.; van de Mosselaar, M.; Rutten, P.; Choenni, S. On Using Privacy Labels for Visualizing the Privacy Practice of SMEs: Challenges and Research Directions. In Proceedings of the DGO 2022: The 23rd Annual International Conference on Digital Government Research, Virtual Event, 15–17 June 2022; pp. 166–175.
13. Feasey, R.; de Streel, A. Data Sharing for Digital Markets Contestability: Towards a Governance Framework; Centre on Regulation in Europe asbl (CERRE): Brussels, Belgium, 2020.
14. Mohan, J.; Wasserman, M.; Chidambaram, V. Analyzing GDPR Compliance through the Lens of Privacy Policy. In Heterogeneous Data Management, Polystores, and Analytics for Healthcare, Proceedings of the VLDB 2019 Workshops, Poly and DMAH, Los Angeles, CA, USA, 30 August 2019; Springer: Cham, Switzerland, 2019; pp. 82–95.
15. Schwaig, K.S.; Kane, G.C.; Storey, V.C. Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? Inf. Manag. 2006, 43, 805–820.
16. Zaeem, R.N.; German, R.L.; Barber, K.S. Privacycheck: Automatic summarization of privacy policies using data mining. ACM Trans. Internet Technol. TOIT 2018, 18, 1–18.

17. McDonald, A.M.; Cranor, L.F. The cost of reading privacy policies. Isjlp 2008, 4, 543.
18. Griggio, C.F.; Nouwens, M.; Klokmose, C.N. Caught in the Network: The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems. In Proceedings of the CHI '22: Conference on Human Factors in Computing Systems, New Orleans, LA, USA, 29 April–5 May 2022; pp. 1–23.
19. Reisinger, T.; Wagner, I.; Boiten, E.A. Security and privacy in unified communication. ACM Comput. Surv. CSUR 2022, 55, 1–36.
20. Andreou, A.; Goga, O.; Loiseau, P. Identity vs. attribute disclosure risks for users with multiple social profiles. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney, Australia, 31 July–3 August 2017; pp. 163–170.
21. Hittmeir, M.; Mayer, R.; Ekelhart, A. A baseline for attribute disclosure risk in synthetic data. In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, 16–18 March 2020; pp. 133–143.
22. Li, N.; Qardaji, W.; Su, D.; Wu, Y.; Yang, W. Membership privacy: A unifying framework for privacy definitions. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 889–900.
23. Hayes, A. Business. Available online: https://www.investopedia.com/terms/b/business.asp (accessed on 22 February 2022).
24. Kenton, W. Third Party. Available online: https://www.investopedia.com/terms/t/third-party.asp (accessed on 22 February 2022).
25. Kenton, W. Customer. Available online: https://www.investopedia.com/terms/c/customer.asp (accessed on 22 February 2022).
26. Chen, J. Business-to-Business. Available online: https://www.investopedia.com/terms/b/btob.asp (accessed on 22 February 2022).
27. Lucking-Reiley, D.; Spulber, D.F. Business-to-business electronic commerce. J. Econ. Perspect. 2001, 15, 55–68.
28. Tamplin, T. Business to Consumer (B2C) Meaning. Available online: https://learn.financestrategists.com/finance-terms/b2c/ (accessed on 11 March 2022).
29. Norris, J. Types of Customer Data: Definitions, Value, Examples. Available online: https://www.the-future-of-commerce.com/2021/04/23/types-of-customer-data-definition-examples/ (accessed on 11 March 2022).
30. Freedman, M. How Businesses Are Collecting Data (And What They're Doing with It). Available online: https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (accessed on 11 March 2022).
31. Pearson, S.; Benameur, A. Privacy, security and trust issues arising from cloud computing. In Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, 30 November–3 December 2010; pp. 693–702.
32. Greenaway, K.E.; Chan, Y.E.; Crossler, R.E. Company information privacy orientation: A conceptual framework. Inf. Syst. J. 2015, 25, 579–606.
33. Chinchih, C.; Frey, C.B.; Presidente, G. Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally; Oxford Martin School: Oxford, UK, 2022.
34. Sun, Y.; Lo, F.P.-W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access 2019, 7, 183339–183355.
35. Davari, M.; Bertino, E. Access control model extensions to support data privacy protection based on GDPR. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 4017–4024.
36. Wolford, B. GDPR Compliance Checklist for US Companies. Available online: https://gdpr.eu/compliance-checklist-us-companies/ (accessed on 29 September 2023).
37. ABS Five Safes Framework. Available online: https://www.abs.gov.au/about/data-services/data-confidentiality-guide/five-safes-framework (accessed on 23 September 2023).