Article

OECD-Driven Operational Risk Management for Personal Data Safeguarding

António Gonçalves [1,2]*, Anacleto Correia [1]

[1] CINAV

[2] INESC-ID

***** Correspondence: **agoncalveslx@gmail.com**

Abstract: The article examines the "Guidelines for the Protection of Privacy and Transborder Flows of Personal Data" by the OECD, proposing a model that incorporates its recommendations to evaluate and improve compliance with data protection regulations. By employing the Object-Role Modeling (ORM) methodology, the study develops a detailed representation of the relationships and constraints between entities such as Data Controller and Personal Data, emphasizing transparency, accountability, and interoperability. Finally, it suggests transforming the ORM model into first-order logic to enhance formal analysis and automate reasoning. The article highlights the benefits in terms of clarity, precision, and the identification of inconsistencies, aiming to strengthen the privacy and security of personal data.

Keywords: privacy; personal data; interoperability; modeling

1. Introduction

The OECD Council's Recommendations, encapsulated in the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," [1] serve as a foundational framework aimed at bolstering the protection of personal data privacy on a global scale. These guidelines are instrumental in setting universal standards that seek to balance the free flow of information across borders with the imperative need to safeguard personal privacy. The emphasis is on crafting a robust structure that enables data to move freely and securely, thus facilitating international commerce and communication, while simultaneously ensuring that individuals' privacy rights are respected and protected.

Central to these guidelines are eight critical principles designed to guide the collection, processing, and management of personal data [1]. These include the limitation of data collection, ensuring data quality, specifying the purpose of data collection, limiting the use of data, implementing security safeguards, maintaining transparency, facilitating individual participation, and enforcing accountability.

Each principle serves as a cornerstone in the architecture of data privacy, ensuring that personal data is handled with the utmost care and responsibility. Collectively, they provide a comprehensive approach to data protection, ensuring that personal information is collected and used ethically, securely, and in a manner that respects individual rights and freedoms.

Furthermore, these recommendations emphasize the importance of international cooperation and interoperability in the context of personal data privacy. They call for measures to facilitate cooperation in the enforcement of privacy laws and the development of international agreements that promote interoperability between privacy frameworks.

The objective of this study is to develop a model that captures the essence of the OECD Council's recommendations and can be used as a reference to analyze different data protection regulation implementations, allowing for a consistent evaluation of data protection practices in compliance with the OECD guidelines. The aim is to contribute to strengthening privacy and personal data security, ensuring compliance with legal requirements, and promoting a culture of accountability and transparency through the promotion of interoperability among various data protection regulations concerning the OECD Council's recommendations on Personal Data Privacy Protection.

This study is designed with a forward-looking approach, aiming to not just satisfy the existing requirements for data protection but to also preemptively tackle emerging challenges in the realm of digital privacy and the safeguarding of individual rights and freedoms. By exploring strategic methodologies for managing data protection, this research aspires to provide organizations with a robust framework that not only aligns with current legal mandates but is also adaptable to future changes in the digital landscape. This involves a comprehensive analysis of potential shifts in regulatory environments, technological advancements, and societal expectations regarding privacy, ensuring that organizations are well-prepared to protect individual data rights proactively in an ever-evolving digital context.

In this regard, this study seeks to answer the following research question: What strategies can multinational organizations adopt to harmonize internal procedures and ensure simultaneous compliance with multiple privacy regulations?

The document is structured as follows: It begins with a literature review in section II, establishing the theoretical context through related works. Section III details the methodology and components of the model, clarifying its construction and theoretical foundation. The presentation of the proposed solution occurs in section IV, where its main characteristics are elucidated. The discussion on the applicability and effectiveness of the model in various contexts is carried out in section V, evaluating its robustness and potential limitations, as well as reflecting on the positive impact on personal data protection. It concludes by suggesting directions for future research.

2. Related work

The protection of personal data has emerged as a central theme in the digital age, reflecting a significant transformation of laws and regulations globally. This evolution, as mentioned by Phillips [2], has been particularly influenced by the Guidelines of the Organisation for Economic Co-operation and Development (OECD) and the European Union's General Data Protection Regulation (GDPR), marking a new paradigm in how privacy is perceived and managed.

The OECD guidelines, initially set in 1980 and revised in 2013, represented one of the first international reference frameworks, instituting foundational principles such as data collection limitation, data quality, and information security. These principles aim to ensure that personal data is processed fairly, transparently, and with proper protection. Their influence is particularly notable in the design of the GDPR, which, since its implementation in 2018, has established new standards for data protection in Europe, highlighting the rights of data subjects, transparency in operations, and the accountability of data processors.

The historical development of data protection legislation, meticulously analyzed by Babikian [3], traces a significant evolution from early regional agreements and international treaties to the formulation of comprehensive national laws. This evolutionary path highlights an increasing global consciousness regarding the paramount importance of privacy in our interconnected world. It reflects a collective awakening to the idea that the protection of personal information is not just a matter of individual interest but a fundamental human right that underpins the very essence of democracy and personal freedom. As Babikian's work suggests, the shift towards detailed national laws signifies a recognition by governments and policymakers of the nuanced challenges presented by the digital age. This includes not only the risks posed by unauthorized access and misuse of personal data but also the broader implications for autonomy, freedom of expression, and the right to be forgotten. The progression from broad principles to specific, enforceable statutes illustrates an effort to create robust legal frameworks capable of safeguarding individuals against the invasive capabilities of modern technology while promoting transparency, accountability, and trust between data subjects and controllers.

A pivotal element within the realm of data protection is the principle of informed consent, a notion underscored by Behrendt [4], particularly in the spheres of medicine and research. This principle transcends mere legal obligation, crystallizing as a cornerstone ethical tenet that safeguards individual autonomy and underpins the legitimacy of data processing activities. Informed consent is foundational, ensuring that individuals are fully aware and voluntarily agree to the processing of their personal data, thereby acknowledging and respecting their rights and decision-making capabilities. This approach not only reinforces the ethical integrity of data handling practices but also enhances trust and transparency between data subjects and entities, making it a critical aspect of data protection that goes beyond regulatory compliance to embody a commitment to respect and protect personal autonomy in the digital age.

However, the effectiveness of data protection regulations is sometimes compromised by the ambiguity of the terms used. The lack of a universally recognized definition of "data privacy," as indicated by Covert [5], can lead to inadequate protections and uneven application of laws. This ambiguity highlights the need for a more solid consensus on the fundamental concepts of privacy and data protection.

The emergence of artificial intelligence (AI) has introduced new challenges and possibilities for compliance with data protection regulations. The distinction between rule-based technologies and machine learning systems, highlighted by Kingston [6], underscores the

importance of detailed knowledge representation and a clear justification of decisions made by AI systems to ensure transparency and compliance.

To address the complexity of compliance, Lambrinoudakis [7] suggests a series of principles, including organizational preparedness, maintaining records of processing activities, and appointing a data protection officer. These principles provide a foundation upon which organizations can adapt their practices to ensure effective protection of personal data.

Additionally, challenges related to accessing personal data are exacerbated by the variety of contexts in which data is collected and processed. Grundstrom [8] identifies these challenges in four main areas: procedure, protection, privacy, and dispersion, emphasizing the inherent complexity in managing personal data and the need for holistic approaches to ensure compliance and protect individuals' privacy.

In concluding, it's essential to recognize that the trajectory of data protection laws is inherently intertwined with the interplay of advancing technology, societal norms, and legal frameworks. This triad operates in a fluid, ever-changing landscape where each component influences and is influenced by the others. As we navigate through this evolving terrain, there emerges a critical demand for approaches that are not only transparent and ethical but also deeply rooted in a sound understanding of the complexities at play. Such strategies must consider the rapid pace of technological innovation, the shifting sands of social expectations regarding privacy, and the increasingly intricate tapestry of legal requirements across jurisdictions.

This necessitates a sustained effort and unwavering commitment from all stakeholders involved, including governments, private entities, civil society, and individuals. The goal is to foster a digital ecosystem that upholds the dignity and privacy of individuals while accommodating the growth and innovation that technology brings. Achieving this balance requires ongoing dialogue, collaboration, and adaptation to ensure that data protection measures are effective, equitable, and reflective of our collective values and aspirations. As we move forward, the ability of organizations to anticipate changes, engage in ethical data practices, and demonstrate a commitment to the principles of data protection will be paramount in navigating the complexities of the digital age.

3. Methodology

To conduct the compliance assessment, terminology mapping is an essential activity, involving the mapping of organizations' personal data protection policies to the concepts used in the OECD Guidelines for the Protection of Privacy. The terminology should be mapped at the beginning of the policy drafting phase of an organization based on the OECD directives. However, for practical reasons, we are dealing with existing organizations whose policies were specified without considering the regulations. Therefore, a condition for terminology mapping is the correct capture of the ontology of the terminology concepts of the OECD Privacy Protection guidelines.

For this purpose, it is necessary to choose a tool that allows modelling, and the Object-Role Modelling (ORM) method has been adopted [9].

ORM stands as a sophisticated technique for conceptual modelling, pivotal in the realm of database and software design. This approach is distinctive for its use of natural language to articulate the requirements of a system, thereby encapsulating the essential facts that delineate objects (entities) and the roles they play within various relationships. By employing natural language, ORM facilitates a deeper, intuitive understanding of the model's structure, making it accessible not only to developers and database designers but also to stakeholders and business analysts who may not be deeply versed in technical specifications.

At the heart of ORM is its focus on the semantics of the data model, emphasizing the importance of accurately representing real-world phenomena in a way that mirrors human understanding and communication. This method involves identifying the entities that exist within a system and describing the dynamic interactions between these entities through facts. These facts, articulated in a clear and straightforward manner, serve as the building blocks for constructing a comprehensive picture of the system's data architecture.

Furthermore, ORM promotes a high degree of precision and validation in modelling, encouraging the explicit specification of constraints and rules governing the relationships between objects. This precision ensures that the resulting database or software system aligns closely with the actual operational and informational needs of the organization.

By bridging the gap between technical design and business logic, ORM empowers stakeholders to engage more directly with the modelling process. This collaborative approach enhances the quality of the final system design, ensuring that it is both technically sound and closely aligned with business objectives and user needs. As a result, ORM stands as a valuable tool in the development of complex data-driven systems, offering a clear, understandable, and rigorous method for capturing the intricacies of real-world data relationships.

ORM is a concept modelling technique that describes requirements through facts. Each fact in ORM is structured to convey a specific piece of information about how objects (entities) relate to each other within the system's context. This is achieved by identifying roles that objects play in their interactions, which are then expressed in easily understandable sentences. For example, a fact in an ORM model might state, "A customer places an order," where "customer" and "order" are objects, and "places" describes their relationship.

All facts are treated as instances of attribute-free structures known as fact types, which are devoid of attributes and focus solely on the relationships between objects. These fact types are categorized based on the complexity of the relationships they describe, ranging from unary (involving a single entity in a specific role, such as "Person is employed"), to binary (involving two entities in a relationship, such as "Person works at Company"), and extending to more complex relational structures that involve multiple entities and roles.

Unary fact types describe a condition or a state of a single entity, essentially capturing properties of individual objects in a way that is naturally expressed and understood. For example, a unary fact type could represent whether a "Person is eligible for retirement," focusing solely on the state or characteristic of the person.

Binary fact types, on the other hand, establish a direct relationship between two entities, making it clear how one object relates to another. This simplicity and directness make binary relationships particularly straightforward for natural language expression and understanding. An example of a binary fact type is "Person owns Car," which clearly indicates the relationship between a person and a car.

For more complex scenarios involving multiple entities and relationships, ORM allows for the definition of fact types that encapsulate these intricate interactions. Despite their complexity, these fact types are still designed to be expressed in natural language, ensuring that the model remains accessible and comprehensible. An example of a more complex fact type could be "Employee works on Project under Manager," which involves multiple roles and relationships within a single fact type.

In extracting information from the OECD regulation to develop an ORM model, the method proposed by Cockburn [10], was used, as it allows following a structured and user-centered approach. This enables a deep understanding of the users' needs and the system's usage contexts, essential for identifying entities, roles, and relationships in the ORM model.

The process of transforming the OECD standard describing data protection principles into an ORM model follows a structured methodology. Initially, a detailed analysis of the text is carried out to identify and extract fundamental concepts that translate into objects or entities in the ORM model, such as 'Data Controller', 'Personal Data', 'Data Subject', among others. This stage involves a deep understanding of the domain in question and the identification of key elements that will form the basis of the model.

Subsequently, the interactions and relationships between the identified objects are examined, determining the roles each plays. For example, a 'Data Controller' may 'collect' or 'use' 'Personal Data'. These relationships are mapped according to the verbs and actions described in the text, paying special attention to nuances and legal implications that may influence the nature of the relationships.

Furthermore, the restrictions and conditions implicitly or explicitly mentioned in the text, such as limitations on data collection and use, consent requirements, and security obligations, are analysed. These restrictions are fundamental to the model's fidelity to the original principles, ensuring that the ORM model adequately reflects the established norms and guidelines.

4. Modelling

For the purposes of modelling, an analysis of the OECD standard was conducted, identifying eight privacy principles, listed in Table 1 and described below.

Table 1. OECD privacy framework principles.

#	***Principles***
1	Collection Limitation
2	Data Quality Purpose
3	Purpose Specification
4	Use Limitation
5	Data Security
6	Transparency
7	Individual Participation
8	Accountability

1. **Principle of Collection Limitation:** Personal data should be obtained by lawful and fair means, and where appropriate, with the knowledge or consent of the individual.

2. **Principle of Data Quality:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-dates.

3. **Principle of Purpose Specification:** The purposes for which personal data are collected should be specified not later than at the time of data collection. The subsequent use is limited to the fulfillment of those purposes or such others as are not incompatible with the original purposes and as specified at the time of collection.

4. **Principle of Use Limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes except a) with the consent of the data subject or b) by the authority of law.

5. **Principle of Security:** Adequate protection should be ensured for personal data against risks such as loss, unauthorized access, destruction, use, modification, or disclosure of data.

6. **Principle of Transparency:** There should be a general policy of transparency about the use of personal data. This means it should be possible for an individual to ascertain the existence and nature of the data, the main purposes of its use, as well as the identity and usual residence of the data controller..

7. **Principle of Individual Participation:** An individual should have the right to: a) obtain from a data controller confirmation of whether or not the controller has data relating to him; b) have communicated to him such data within a reasonable time and at a charge that is not excessive; c) challenge data and, if the challenge is successful, to have the data erased, rectified, completed, or amended..

8. **Principle of Accountability**: Data controllers should be accountable for complying with measures which give effect to the principles stated above..

ORM Modeling

Objetc/Entity:

1) Data Controller
2) Personal Data
3) Data Subject
4) Purposes
5) Data Protection Authority

Relationships and Roles:

1) **Data Controller - Personal Data**

   a) **Roles:** "collects", "uses"
   b) **Restrictions:** Collection must be limited, lawful, and fair; use must be secure and in accordance with specified purposes.

2) **Personal Data - Data Subject**

   a) **Roles:** "relate to"
   b) **Restrictions:** There must be consent or knowledge of the data subject for collection and use.

3) **Personal Data – Purposes**

   a) **Roles:** "are collected for", "are used for"
   b) **Restrictions:** Purposes must be specified at collection and adhered to subsequently.

4) **Data Controller - Data Protection Authority**

   a) **Roles:** "is regulated by"
   b) Restrictions: The data controller must comply with security measures and be accountable to the authority.

5) **Data Subject - Data Controller**

   a) **Roles:** "has rights over"
   b) **Restrictions:** Includes the right of access, rectification, and objection.

Application of Restrictions and Conditions:

a) **Collection Limitation:** Personal Data should not be excessively collected and must be obtained in a lawful and fair manner.

b) **Data Quality:** Personal Data must be accurate, complete, and updated as necessary.

c) **Purpose Specification:** The purposes for collecting Personal Data must be clearly defined and communicated.

d) **Use Limitation:** The use of Personal Data is limited to the specified purposes, unless explicit consent from the data subject or legal authorization exists.

e) **Security Safeguards:** Adequate protection must be ensured against risks such as loss, unauthorized access, and others.

f) **Openness:** There should be a general policy of openness about the handling of Personal Data.

g) **Individual Participation:** Data subjects should be able to access and correct their data and challenge its processing.

h) **Accountability:** The Data Controller must be responsible for ensuring adherence to these rules.

This ORM model abstracts and represents the relationships between the identified entities and privacy principles, illustrating how personal data is collected, used, and managed, as well as the rights of the data subject and the obligations of the data controller. The applied restrictions ensure compliance with data protection principles, providing a clear basis for the responsible and secure handling of personal information.

5. Conclusions and Future Work

The conducted study concludes that developing a model based on the standards established by the Organisation for Economic Co-operation and Development (OECD) provides a strong foundation for analyzing an organization's compliance with privacy regulations, irrespective of the specific regulatory framework it adheres to.

Adherence to the OECD guidelines significantly increases the likelihood that an organization will meet the requirements of other privacy standards across various regions. This stems from the fact that the OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data encapsulate core data protection principles that are broadly recognized and implemented globally.

Consequently, organizations that align their internal policies and procedures with the OECD guidelines not only demonstrate a commitment to achieving a high level of personal data protection but also enhance their ability to adapt to and comply with diverse privacy regulations more effectively and consistently.

Future work could involve transforming this ORM model into a first-order logic representation, which would further amplify the benefits of modeling. First-order logic, as a more formal and mathematical framework, enables the application of automatic reasoning techniques and consistency verification. Entities, relationships, and constraints within the

ORM model could be converted into logical formulas that precisely and unambiguously represent the knowledge embodied in the standard.

This transformation would support the development of information systems capable of automatically verifying compliance with standards, identifying potential conflicts or logical inconsistencies, and generating inferences based on available data. Additionally, first-order logic representations could be applied in decision support systems, predictive analytics, and knowledge integration from multiple sources, thereby improving the efficiency and effectiveness of norm-based decision-making processes.

References

[1] OECD, "THE OECD PRIVACY FRAMEWORK 2013," 2013.

[2] M. Phillips, "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)," Hum. Genet., vol. 137, no. 8, pp. 575–582, 2018.

[3] J. Babikian, "Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era," Law Res. J., vol. 1, no. 2, pp. 91–101, 2023.

[4] C. A. Behrendt, A. Joassart Ir, E. S. Debus, and P. Kolh, "The Challenge of Data Privacy Compliant Registry Based Research," Eur. J. Vasc. Endovasc. Surg., vol. 55, no. 5, pp. 601–602, 2018.

[5] Q. Covert, M. Francis, D. Steinhagen, and K. Streff, "Towards a triad for data privacy," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2020-Janua, pp. 4379–4387, 2020.

[6] J. Kingsto, "Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation," Artif. Intell. Law, vol. 25, no. 4, pp. 429–443, 2017.

[7] C. Lambrinoudakis, "The General Data Protection Regulation (GDPR) Era : Ten Steps for Compliance of Data Processors and Data Controllers," in Trust, Privacy and Security in Digital Business, Springer International Publishing, 2018, pp. 3–8.

[8] C. Grundstrom, K. Väyrynen, N. Iivari, and M. Isomursu, "Making sense of the general data protection regulation-four categories of personal data access challenges," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2019-Janua, pp. 5039–5048, 2019.

[9] T. Halpin, Object-Role Modeling Fundamentals: A Practical Guide to Data Modeling with ORM. 2015.

[10] A. Cockburn and Lord Cockburn, Writing effective use cases. Pearson Education, 2015.