AXIOLOGIC

Data Privacy Management Obligations

Author: Alboaie Sînică
Date: August 2023
Version: v 1.0

1. Purpose....3
1.1 Introduction....3
1.2 Scope of Guidelines....3
1.3 Objective....3
1.4 Benefits....3
1.5 Review and Updates....4
2. Code of conduct....5
2.1 Adherence to GDPR Privacy Principles....5
2.2 Privacy and Security by Design and Default....5
2.3 No Processing of Sensitive Privacy Data in Vendor Services....6
2.4 General Policy....6
3. Standard Contractual Clauses....7
3.1 Employee Responsibilities....7
3.2 Inclusion in Commercial Contracts....7
3.3 Scope of Standard Contractual Clauses....8
3.4 Review and Amendment....8

4. Data Protection Officer **9**
4.1 Designation of Representative 9
4.2 Technical and Organizational Measures 9
4.3 Personal Data Breach Notification 9
4.4 Default Designation of Data Protection Officer (DPO) 9
4.5 Delegation of DPO Responsibilities 9
4.6 Accountability and Reporting 10
5. Publicly available privacy policy/notice **10**
6. Record-keeping process **10**
7. Employee onboarding process **11**
8. Data Privacy Frameworks & Timelines **12**
9. Conclusions and Summary **12**

1. Purpose

1.1 Introduction

This document aims to establish and articulate the data privacy management obligations that Axiologic Research ("the Company") is committed to uphold. With the increasing importance and scrutiny of personal data protection, it is imperative for the Company to consistently meet both legal and ethical standards in handling personal data.

1.2 Scope of Guidelines

This document outlines the Company's position and approach to managing several key aspects of data privacy, which include but are not limited to:

Standard Contractual Clauses: Ensuring that any data transfer mechanisms the Company uses, particularly across borders, are secure and comply with the relevant data protection laws. This includes using Standard Contractual Clauses where necessary to safeguard data transfers.

Publicly Available Privacy Policy/Notice: Maintaining a clear, accessible, and comprehensive privacy policy that informs stakeholders – including customers, employees, and partners – of how their data is being used, stored, and protected by the Company.

Record of All Categories of Processing Activities: Keeping a detailed and up-to-date record of all data processing activities undertaken by the Company, as required under relevant data protection laws. This includes the categories of data processed, the purpose of processing, and the parties with whom data is shared.

Privacy By Design and Security By Design: Integrating data protection into every stage of the Company's product and process development. This includes taking proactive steps to identify and mitigate risks to personal data from the outset rather than retroactively.

Employee Onboarding Process: Ensuring all employees are educated about their roles and responsibilities in protecting personal data as part of their onboarding process and are trained on the Company's data protection policies and procedures.

Data Protection Officer Responsibilities: Clearly defining the role, responsibilities, and authority of the Data Protection Officer (DPO), who oversees the Company's data protection strategy and its implementation to ensure compliance with relevant laws and regulations.

1.3 Objective

The primary objective of this document is to provide a robust and actionable framework for Axiologic Research to effectively manage and secure personal data by the law and best practices. It aims to foster a culture of respect for personal data and continual improvement in data protection practices within the Company.

1.4 Benefits

Axiologic Research aims to demonstrate a commitment to responsible data management by adhering to these guidelines. The company seeks to build trust with stakeholders, including customers, employees, and partners. These guidelines are designed to reduce the risk of data breaches and minimise

legal and reputational damage. Additionally, they help Axiologic Research to ensure compliance with evolving global data protection regulations.

1.5 Review and Updates

This document will be a living resource that will be reviewed and updated periodically to reflect changes in legal requirements, technological advancements, and stakeholders' evolving needs and expectations.

2. Code of conduct

2.1 Adherence to GDPR Privacy Principles

Axiologic Research (“the Company”) is committed to adhering to the GDPR Privacy Principles (General Data Protection Regulation (GDPR) is a comprehensive data protection regulation that the European Union adopted). As a vendor offering software development and research services, the Company maintains a rigorous standard of data protection that aligns with the lawful, fair, and transparent processing of personal data. Specifically, the Company is committed to:

- Lawfulness, Fairness, and Transparency: The Company ensures that personal data is processed legally, fairly, and transparently about the data subject.
- Purpose Limitation: The Company collects personal data for specified, explicit, and legitimate purposes and does not process it further in an incompatible manner.
- Data Minimization: In line with the ‘Privacy by Design’ principle, the Company only processes data necessary for the intended purpose and avoids collecting excessive information.
- Accuracy: The Company takes reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date; it takes steps to rectify or erase inaccurate data without delay.
- Storage Limitation: The Company retains personal data for no longer than is necessary for the purposes for which the data is processed.
- Integrity and Confidentiality (Security): The Company implements appropriate technical and organisational measures to ensure a high level of security, protecting personal data against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- Accountability: The Company is responsible for and can demonstrate compliance with these principles. This involves a proactive approach, including regular staff training, audits, and reviews of data processing activities and security measures.
- Rights of the Data Subject: The Company respects and facilitates the exercise of data subject rights under the GDPR, including the right to access, rectification, erasure (“the right to be forgotten”), data portability, restriction of processing, the right to object, and rights about automated decision making and profiling.

By adhering to these principles, Axiologic Research places the highest importance on protecting its clients' and users' data. It continuously seeks to review and improve its data protection protocols and practices to ensure they are effective, robust, and fully compliant with the GDPR.

2.2 Privacy and Security by Design and Default

The Company embeds privacy and security into developing and operating its products and services. By design and by default, data protection measures are integral to product development, not added as an afterthought.

2.3 No Processing of Sensitive Privacy Data in Vendor Services

When working as a vendor, the Company does not process sensitive privacy data unless explicitly specified in the contract with its customers. Sensitive privacy data refers to special categories of personal data, as defined under GDPR.

2.4 General Policy

As a general policy, the Company:

- Strictly adheres to GDPR Privacy Principles when processing personal data.
- Employs 'Privacy and Security by Design and Default' principles in all product development and research stages.
- Does not process sensitive privacy data in its capacity as a vendor unless explicitly specified and agreed upon in the contract with its customers.

2.5 Specific Customer Contracts and Internal Projects

For other internal projects, or when explicitly specified in the contract with customers, the Company may process private data strictly following GDPR. This includes obtaining necessary consent, safeguarding the data rights of the subjects, and ensuring lawful processing grounds.

2.6 Vendor Responsibility

Vendors and third-party partners engaged by the Company are expected to respect and comply with the Company's privacy standards. They must align with the GDP Privacy Principles and GDPR and adhere to the specific terms in their contracts regarding data processing.

2.7 Enforcement and Accountability

The Company holds itself accountable for adhering to the principles and practices outlined in this Code of Conduct. Non-compliance with this Code, or with specific terms set out in contracts with customers or vendors, is treated seriously and may result in disciplinary action, including termination of employment or contractual relationships.

3. Standard Contractual Clauses

3.1 Employee Responsibilities

Axiologic Research ("the Company") requires all employees to strictly adhere to the Company's Data Privacy Management Obligations. These obligations outline the measures and conduct expected from every member of the Axiologic team to ensure data privacy and security are maintained at all times. Employees are required to:

- Familiarise themselves with, and have a thorough understanding of, the Data Privacy Management Obligations.
- As provided by the Company, engage in regular training sessions on data protection and privacy.
- Immediately report any data breaches or suspected breaches to the designated Data Protection Officer (DPO) or relevant authority within the Company.
- Follow all data protection protocols and practices outlined in the Data Privacy Management Obligations in their day-to-day activities and interactions with data.

At Axiologic Research, employees are entrusted with a multi-faceted responsibility, from ensuring top-notch security protocols to maintaining the sanctity of private data and safeguarding commercial secrets. The same stringent standards apply when working as a vendor for external clients or on internal projects. Employees are expected to exercise vigilance and adhere to best practices in security, consistently updating passwords and utilising secure and encrypted channels for communication.

In private data protection, they are mandated to access only the data necessary for their tasks, thus embodying the principle of ‘data minimisation.’ They are educated to recognise the sensitive nature of personal data and are trained to handle such information with the utmost care and discretion.

Understanding the ramifications of data breaches, employees at Axiologic Research are prompt in reporting any suspicious activities or security vulnerabilities they detect. They are committed to not storing data on unauthorised devices and are vigilant about securing their workstations when they are away, even temporarily.

Preserving commercial secrets holds equal weight. Whether in dealings with clients when Axiologic acts as a vendor or during internal projects, employees are strictly obligated not to disclose, share, or misuse proprietary information. This includes but is not limited to, algorithms, source codes, and business strategies that are integral to Axiologic’s competitive edge.

Additionally, employees maintain a professional demeanour when communicating with clients, ensuring that they uphold Axiologic’s reputation by not disclosing confidential or sensitive information unless explicitly authorised. The sanctity of contracts, encompassing all clauses and stipulations that pertain to data handling, security, and confidentiality, is treated by employees as sacrosanct.

Furthermore, employees are expected to remain current with the latest trends and best practices in data protection and security through continuous education, aligning their daily operations with the evolving landscape of data protection regulations.

In summary, at Axiologic Research, every employee is a steward of data protection, security, and commercial confidentiality, continually upholding these values as they navigate the complexities of both vendor relationships and internal operations.

3.2 Inclusion in Commercial Contracts

As part of its commitment to upholding data privacy, Axiologic ensures that a summary of its Data Privacy Management Obligations is incorporated into all commercial contracts with customers or suppliers. This summary will:

- Clearly outline the expectations and responsibilities of both parties regarding data privacy and security.
- Affirm Axiologic's commitment to safeguarding personal and sensitive data by relevant data protection laws and its stringent standards.
- Specify the legal and contractual consequences for any breach of these data privacy and security obligations.

3.3 Scope of Standard Contractual Clauses

These Standard Contractual Clauses are designed to provide a strong, enforceable framework that ensures:

- Compliance with relevant data protection legislation.
- The rights of data subjects are protected and upheld.
- Axiologic and its contracting parties (customers or suppliers) are held to the same high data privacy and security standards.

3.4 Review and Amendment

To ensure that the Standard Contractual Clauses remain compliant with evolving data protection regulations, Axiologic is committed to the following:

- Regularly reviewing and, if necessary, updating these clauses.
- Communicating any amendments to relevant parties in a timely and transparent manner.

3.5 Enforcement and Accountability

Failure to comply with the responsibilities and obligations outlined in the Standard Contractual Clauses may result in significant consequences. These may include:

- Legal action is being taken against the non-compliant party.
- Immediate termination of the commercial contract in question.
- Potential fines and penalties as prescribed by relevant data protection legislation.

4. Data Protection Officer

4.1 Designation of Representative

As a vendor, Axiologic Research ("the Company") provides evidence of the designation of a representative in the jurisdiction where the applicable data protection law(s) are in force. This ensures the Company is accountable and reachable by data subjects and data protection authorities in that jurisdiction.

4.2 Technical and Organizational Measures

The Company, as a vendor, is committed to implementing appropriate technical and organisational measures designed to ensure a level of security that is appropriate to the risk to individuals. These measures aim to prevent unauthorised access, disclosure, alteration, and destruction of personal data. Regular audits and assessments are performed to evaluate and improve data security controls. Under this policy, an internal audit will be conducted at least once every three months or when an important event or situation necessitates a review. The results of each internal audit will be recorded in the journal described in Chapter 6 of this document.

4.3 Personal Data Breach Notification

Axiologic Research has stringent policies and procedures and commits to notify its clients immediately after becoming aware of a personal data breach or security incident. This rapid response is vital to minimise potential harm to data subjects and comply with legal obligations.

4.4 Default Designation of Data Protection Officer (DPO)

By default, the Data Protection Officer (DPO) of Axiologic Research is the Axiologic Research Administrator. The DPO oversees the company's data protection activities and ensures compliance with relevant laws. This individual serves as the liaison between the company and applicable data protection authorities and is tasked with educating employees on compliance requirements while training them in implementing data protection policies.

4.5 Delegation of DPO Responsibilities

The Axiologic Research Administrator, as the default DPO, has the authority to delegate the responsibilities of the DPO role to another individual within the organisation through an internal decision. Such delegation will be formally documented, and the designated individual will possess the necessary knowledge, experience, and skills to assume the role and responsibilities of the DPO effectively.
The delegation of Data Protection Officer (DPO) authorities is permissible, provided that the designated individual complies rigorously with the segregation of duties requirements stipulated in Articles 37-39 of the General Data Protection Regulation (GDPR). This ensures that the role of the DPO remains independent and free from conflicts of interest, thereby upholding the integrity and effectiveness of data protection operations within the Company.

4.6 Accountability and Reporting

The DPO, whether the Axiologic Research Administrator or a delegated individual, must regularly report to the highest management level of the Company on data protection activities and compliance status. This ensures senior management is informed and engaged with the Company's data protection responsibilities.

5. Publicly available privacy policy/notice

This document must be published on www.axiologic.net site.

6. Record-keeping process

To initiate the comprehensive management of data processing activities, Axiologic begins by creating a continuously updated record as processes change or are added. The processed data is then classified as Customer, Employee, Vendor, and Sensitive. Specific processing activities are documented for each data category, including collection, storage, access, modification, and deletion. Each activity is associated with an individual or department responsible for the processing, clearly identifying data processors.

For all processing activities, Axiologic documents the legal basis under which they are conducted, referencing the relevant applicable laws or regulations. Concurrently, risks associated with each processing activity to data subjects are evaluated and recorded, followed by noting the security measures in place for each data category and how they are designed to mitigate the identified risks. Data transfers, including cross-border transfers, are recorded with specificity, indicating the recipient and legal safeguards involved.

An essential part of this process is the logging of data retention periods. For each data category, Axiologic notes the period for which the data will be stored or the criteria used to determine that period. Regular reviews of the record are scheduled and conducted to ensure it remains up-to-date and reflects current practices. Periodic internal audits of the processing activities record are implemented for accuracy and completeness, and relevant staff members are trained to maintain the record and understand the importance of this responsibility.

A standardised report from the record summarises the processing activities clearly and concisely. By default, this record, or processing activities journal, is considered an internal and confidential company document. However, when acting as a vendor, Axiologic may, upon request and at its discretion, offer this journal to customers to demonstrate its data processing practices and compliance.

Access to the processing activities journal is strictly controlled and restricted to authorised personnel within the company. In the case of a data breach or incident, the journal is updated to include details of the incident and actions taken in response. Regular consultation with legal counsel ensures the record meets all regulatory requirements and obligations. Before finalising, the record undergoes senior management review for sign-off to validate its completeness and accuracy. Ultimately, this journal serves as a tool to assure customers of Axiologic's steadfast commitment to data protection and compliance with relevant regulations when acting as a vendor.

7. Employee onboarding process

New hires undergo an extensive initial training program at the commencement of the Employee Onboarding Process at Axiologic Research. This foundational training will equip them with essential knowledge about the company's policies, processes, and tools, particularly on Data Privacy Management Obligations. They are familiar with Axiologic's approach to data privacy, including understanding the various categories of data processed by the company and their responsibilities in managing this data securely and legally.

One of the key aspects of this initial training is a detailed walkthrough of the Data Privacy Management Obligations document. This ensures that employees understand the critical importance of data privacy from the very outset of their tenure and educates them on the practical implications of these obligations in their daily work. New hires must acknowledge receipt and understanding of this document, affirming their commitment to upholding these standards in all professional conduct.

To ensure that employees' knowledge remains current and comprehensive, ongoing training is conducted in response to any changes in the Data Privacy Management Obligations document. This entails timely communication of updates to all staff members, followed by dedicated training sessions explaining the nature of the changes, the rationale behind them, and the practical steps employees must take to align with these updates.

In addition to these structured training modules, Axiologic maintains a robust culture of continuous learning through its weekly internal training and code review sessions. These sessions, often led by experienced team members or external experts, cover many topics, with frequent emphases on security and privacy. These weekly meetings serve multiple purposes: they reinforce the company's commitment to best practices in security and privacy, promote a culture of peer review and collaborative learning, and ensure that the entire team remains informed of the latest trends, threats, and best practices in the rapidly evolving fields of data security and privacy.

Moreover, these weekly sessions are not merely informational; they are interactive and designed to be practical. Employees are encouraged to ask questions, share experiences, and propose solutions, fostering an environment where learning is a shared responsibility and security and privacy are seen not as checkboxes but as integral to the company's operations and reputation.

This continuous loop of initial training, adaptive learning due to changes in critical documents, and ongoing, focused weekly sessions ensures that every Axiologic Research employee, from the newest hire to the most seasoned veteran, is not only aware of their responsibilities concerning data privacy but is also equipped with the knowledge and skills necessary to execute those responsibilities effectively.

All Axiologic Research employees must sign the documents mandated by Romanian and European employment legislation when hiring. This includes internal regulations, such as the company's internal order regulations, and various declarations that reflect their legal responsibilities as employees. These documents outline the rules and expectations governing workplace behaviour, data handling practices, and general employment conditions, ensuring that all parties know their rights and obligations from the outset. The act of signing these documents is a formal acknowledgement by the employees of their understanding and acceptance of these terms and their commitment to upholding the legal and ethical standards set forth by Axiologic Research in alignment with national and international regulations.

8. Data Privacy Frameworks & Timelines

As of August 2023, the "Data Privacy Management Obligations" document has been officially approved by the leadership of Axiologic Research. In alignment with this pivotal step, the company has concurrently implemented a comprehensive suite of Data Privacy frameworks meticulously designed to operationalise, enhance, and uphold the principles and requirements articulated within this pivotal document. This initiative underscores the company's unwavering commitment to establishing a robust, compliant, and transparent data protection environment in all its operations.

Axiologic Research has strategically implemented three robust Data Privacy frameworks within its organisation, aligning its operations with the highest data protection standards. First, a comprehensive employee training program is designed to educate and continually update the workforce on data privacy principles and best practices, ensuring that all team members can handle sensitive information responsibly and securely. Second, Axiologic maintains a detailed and secure journal to systematically record all relevant data processing activities. While internal to the company by default, this journal can be made available to customers when Axiologic acts as a vendor, promoting transparency and accountability. Third, the company has appointed a dedicated Data Privacy Officer (DPO), as mandated by GDPR. The DPO, who by default is the Axiologic Research Administrator but can delegate responsibilities through an internal decision, serves as the focal point for all data protection activities, ensuring steadfast compliance with GDPR and other relevant data protection laws and acting as the liaison between the company and regulatory authorities. Axiologic Research exemplifies a deep-rooted commitment to data privacy through these three frameworks, making it a core aspect of its organisational culture and business operations.

9. Conclusions and Summary

In the current context, where personal data protection is a global and essential concern, Axiologic Research assumes a proactive role in the field by implementing a rigorous and proactive approach to compliance with data protection standards.

The "Data Privacy Management Obligations" document is the backbone of the company's commitment to data protection. It details the internal processes and policies that ensure compliance with Romanian and European data protection legislation and information security and integrity standards.

Axiologic Research emphasises employees' initial data security and protection training as part of the onboarding process. It continues this commitment through periodic training and code reviews, focusing on safety and confidentiality.

All employees must also sign the necessary documents, following Romanian and European legislation when hiring. These documents, which include internal order regulations and various declarations, highlight employees' legal responsibilities and are a fundamental part of the culture of integrity and compliance promoted by Axiologic.

In conclusion, Axiologic Research demonstrates its deep and ongoing commitment to promoting a work environment that respects and protects personal data, ensuring that its activities remain following the highest ethical and legal standards. This commitment meets legislative requirements and contributes to building trust with its clients, partners, and employees, underscoring its reputation as a responsible and reliable entity in the industry.