Changing finances
for the better.

Information security and Privacy policy

Resume

EOS Matrix is a receivable management company, the first on the market in the Republic of North Macedonia. Our main business activities are collection and redemption of receivables. We are a member of the international group EOS, a leading European provider of financial services outside the banking and insurance sector.

"For a debt-free world" - this is a statement that summarizes the way we work and the reason why we strive to meet the high standards of information security we have.

As part of the EOS Group, we are committed to clearly defined values. We consider the security of personal data as a fundamental right of the individual, and we consider the storage of this data as our duty. Ensuring their integrity, confidentiality and availability is our imperative.

We cooperate with our clients as a service provider, and at the same time as a partner, while we treat the debtors as clients of our clients. We focus on finding solutions that satisfy all stakeholders, while applying the highest standards of information security and personal data protection.

The Information Security and Privacy Policy is a commitment of the Management of EOS Matrix DOOEL - hereinafter "the Company" - to implement, maintain and improve a system for managing privacy and information security. This system ensures the confidentiality, integrity and availability of information related to the operation of the Company, as well as an appropriate degree of security in the collection, processing and transfer of personal data.

The Company monitors processes, information systems and assets on a risk-based approach, taking all technical and organizational measures to protect information assets from internal, external, intentional or unintentional threats in order to ensure that information security and the privacy of individuals are not violated.

The rights of personal data subjects are always respected when collecting and processing data.

In order to confirm its commitment to ensuring privacy and information security as well as the protection of personal data during their processing, the Company has implemented the international ISO 27001 Information Security Management System (ISMS) in 2016, and the ISO 27701 Privacy Information Management System (PIMS) in 2023.

Maintaining information security is a key activity for our success, and at the same time the satisfaction of all stakeholders. To this end, we have chosen to comply with the internationally recognized standards ISO 27001: 2022 and ISO 27701:2019 and their recommendations. Our Data Protection Officer is certified by the international certification body PECB https://pecb.com/en . At the same time, we consistently comply with all legal regulations on data protection in the Republic of N. Macedonia, as well as the recommendations of the parent company.

We manage information security in a way that:

Constantly monitor and upgrade the information security management system,

Constantly monitor and upgrade the privacy information management system,

Control our risks and bring them to an acceptable level,

Provide business continuity,

We are constantly concerned about maintaining a high level of awareness of the importance of information security among our employees.

Strategic goals for information security

- Ensuring the confidentiality, integrity and availability of the data available to the Company
- Respecting the principles of privacy of personal data subjects and ensuring responsibility for the actions taken by each employee of the Company
- Ensuring non-refutation - a legally acceptable belief that the transmitted information was issued and received by the correct, duly authorized entities
- Prevent data loss - reduce the likelihood of data loss and / or leakage of confidential / protected data
- Continuous monitoring and improvement of data processing processes and controls based on a risk-based approach

Principles of privacy and ensuring information security

The Company follows the following principles in order to continuously ensure the privacy and security of information:

- Application of international standards and the existing legislation on data security and archival operations
- Monitoring and implementation of RNM legislation related to information security, such as protection at work, protection of personal data, etc.
- Providing resources for the application of technical measures to ensure a physically secure environment for both data, property and employees.
- Regularly assess the risks to endangering the confidentiality, integrity and availability of information and take measures to reduce them to an acceptable level.
- Preparation of Data Protection Impact Assessment (DPIA) for any new system or process that involves large-scale processing of personal data, processing of sensitive personal data or having a high degree of risk
- Control of access to information.
- Keeping records of the actions that the employees of the Company have taken in the information system of the Company.
- Timely detection and management of incidents and weaknesses in information security through the use of an internal incident reporting system (Incident Management System) as well as regular testing of equipment and information system for vulnerabilities that may occur both internally and from external factor.
- Ensuring business continuity in the operation, for the critical processes of the Company.
- Regular training of employees on personal data protection and information security, in order to ensure employee awareness of this policy and the responsibilities arising from it.

- Application of additional policies, guidelines and rules in the day-to-day operations of the Company that support and complement this policy such as policies for access, classification and management of information, policy for proper use of funds, etc.
- Testing the security of the information system through external certified companies.
- Appoint an Information Security Officer who will coordinate all activities of the information security management system and assign responsibilities to other employees.
- Appointment of a Data Protection Officer who will coordinate all activities of the information privacy management system and the requirements of the Personal Data Protection Law, as well as assigning responsibilities to other employees.

Key results

- The Company will not have unplanned interruptions in the availability of information.
- The integrity and confidentiality of the information will not be compromised.
- Clients and associates will maintain trust in the Company.
- The impact of personal data breach will be limited and reduced to a minimum.

This Information security and Privacy policy is approved by the Company Manager and is subject to annual audit.

Skopje, 12.09.2025

Company for financial consulting and services

EOS Matrix DOOEL Skopje

Chief Executive Officer

Katerina Bosevska Ph.D.