


| | | | |
|--|--|-------------------|------------|
|  EASY DATA INTEGRATION | Personal Data Processing Policy | DOCUMENT CODE: | PDPP_1.0 |
| | | CLASSIFICATION: | C |
| | | EDITION/REVISION: | 1/0 |
| | | DATE: | 17.11.2022 |
| | | PAGES: | 1 / 8 |

PERSONAL DATA PROCESSING POLICY

Contents

| | |
|---|-------------------------------------|
| Description | 3 |
| Scope | 3 |
| Definitions and Vocabulary | 3 |
| Roles and Responsibilities | 3 |
| Top Management of EDI | 3 |
| CISO | Error! Bookmark not defined. |
| Employees | 4 |
| Rights of the data subject according to the Applicable Legislation | 4 |
| Personal Data Processing Activities | 4 |
| Personal data processing activities for the execution of employment contracts | 4 |
| Personal data processing activities for the execution of service contracts with clients | 5 |
| Retention Periods | 5 |
| Retention period of the employee's personal data | 5 |
| Retention period of personal data of client's and partner's employees designated with the execution of the contract | 5 |
| Retention period of personal data of third parties according to the authorization given by the Operator for the execution of the contract | 6 |
| Organizational Measures for the Protection of Personal Data | 6 |
| Technical Measures for the Protection of Employee Data | 7 |
| Transfers to Third-party Organizations and Countries | 8 |
| Communication | 8 |
| Annexes | 8 |

Versioning

| Edition | Revision | Date | Page, Paragraph | Type of revision | Prepared by | Approved by |
|----------------|-----------------|-------------|------------------------|-------------------------|----------------------|---------------------------|
| 1 | 0 | 17.11.2022 | Entire document | Initial draft | Ovidiu Albăstroiu | Mircea-Victor Voiteanu |
| | | | | | | |

Description

The company has adopted this policy to ensure the confidentiality, integrity, and availability of personal data processed by the company.

Scope

This policy applies to all departments, functions, IT systems, and personnel who process personal data within the company.

Foundational Documents

- Law 190/2018
- Regulation 679/2016
- ISO 27001:2022

Definitions and Vocabulary

The company has adopted the definitions and vocabulary from Law 190/2018

Roles and Responsibilities

Top Management of EDI

1. Inventory the personal data processed by the department under their management
2. Inform the CISO of any changes related to the data managed by the department
3. Ensure the implementation of data protection policies and procedures as well as the recommendations of the CISO.

CISO

1. Generally responsible for developing and maintaining the Personal Data Processing Policy and identifying opportunities for continuous improvement.
2. Responsible for informing top management about any necessary changes and identifying opportunities for continuous improvement of the Information Security Management System and data protection.
3. Ensures that the latest version of the policy is distributed and made available to all staff and relevant external parties, as needed.

4. Monitors personal data processing within the company and verifies compliance with security controls.
5. Documents and investigates security incidents involving personal data.
6. Ensures that the company's suppliers comply with the minimum requirements imposed by EDI.
7. Trains staff in the field of personal data protection.

Employees

1. Comply with the company's Policies, Procedures, and security requirements.
2. Comply with the requirements of the Additional Act of the employment contract, regarding personal data.
3. Implement the recommendations of the CISO.

Rights of the data subject according to the Applicable Legislation

1. To request the modification of their personal data held by the Company.
2. To request partial or complete deletion of their personal data held by the Company. This request may lead to the impossibility of continuing the execution of the Employment Contract due to legal requirements or due to the requirements of information security standards for which the Company has been certified. The Company will execute the Employee's request except in cases where this places it in conflict with the law.
3. To request a partial or complete set of their personal data held by the Company.
4. To request assistance from the Company regarding their personal data held by the Company.
5. To be informed when their personal data are requested by other entities such as: public authorities, partners and clients of the Company. The Employee will also be informed of what types of data are requested.
6. To be informed where their personal data are stored, how long they are stored, and what data are stored.
7. The right to receive notifications regarding personal data obtained by the Company through indirect methods, categories of data processed, source of data, and, where applicable, if these data come from public sources.
8. The right to complain to the National Supervisory Authority for Personal Data Processing, the government agency for regulation and monitoring in this field.

Personal Data Processing Activities

Personal data processing activities for the execution of employment contracts

1. Activities for identifying and legally registering the Employee.
2. Communicating with the Employee.
3. Carrying out the Employment Contract, payment of salary and allowances.
4. Compliance and application of physical security policies, information security, data security and confidentiality within the company
5. Evaluating, analyzing and optimizing the activities performed by the Employee
6. Communication between the Employee and the company's clients, partners, suppliers, public authorities, and other third parties
7. Improving efficiency, improving goods and services offered by the Com[any
8. Deleting data after the retention period has expired.

Personal data processing activities for the execution of service contracts with clients

1. Activities for identifying client representatives and signing contracts.
2. Communicating with the client.
3. Execution of contracts
 - a. Processing personal data of third parties, according to the Authorization given by the Personal Data Operator.
 - b. Retention of personal data of third parties, according to the Authorization given by the Personal Data Operator.
 - c. Deletion of personal data of third parties after the contract is terminated, according to the instructions of the Personal Data Operator.

Retention Periods

Retention period of the employee's personal data

a) The duration of the employment contract plus 10 years from the termination of the contractual relationship, according to legal requirements.

Retention period of personal data of client's and partner's employees designated with the execution of the contract

The duration of the service contract plus 1 year from the termination of the contractual relationship. b) The names, phone numbers, and addresses will be kept for the duration of the service contract plus 5 years from the termination of the contractual relationship.

Retention period of personal data of third parties according to the authorization given by the Operator for the execution of the contract

The duration of the service contract plus 2 months from the termination of the contractual relationship. In cases where personal data processing agreements between companies specify other retention periods, these will take precedence.

Organizational Measures for the Protection of Personal Data

1. The company has designated a personal data officer who manages all tasks, policies, processes, and communication regarding GDPR issues, in accordance with Article 39 of the Regulation. The unique contact address can be found below.
2. All staff processing personal data participate in training sessions detailing the necessary procedures for maintaining data security, integrity, and availability, and are notified when changes occur.
3. Once a year, the company conducts an internal audit followed by a management analysis dealing with IT security issues, including those related to personal and sensitive data.
4. To ensure that personal data is kept safe and has not been accessed by unauthorized personnel, we keep the following logs:
 - a. Access attempt logs
 - b. Malware logs
 - c. Event logs
 - d. Administrator and operator logs (actions)
5. Access to personal data is granted to authorized persons, based on the services to be provided as part of the Contract, in accordance with IT security and governance principles, ISO 27001 standard, the principles of least privilege, need to know and of segregation of duties, and in accordance with internal provisions and the access control policy.
6. Employees are contractually obligated to maintain the standards and guidelines for information security and data protection. This applies to temporary staff in the same way. A similar set of obligations is included in agreements with contractors who have access to personal data.
7. Both physical and electronic privileged access accounts (administrators) are limited to a few staff members who are nominated by Management. These privileged roles are reviewed once a year in the Internal Audit.
8. The management of technical vulnerabilities is done according to the testing procedures and directives of the IT Manager. Evaluations, decisions, and responses regarding information security incidents and technical vulnerabilities are described in internal procedures for non-compliance and security incident management.

9. Each employee and contractor is assigned a unique account, with access privileges in accordance with job requirements and best practices recommended by ISO 27001 standard.
10. All staff (including subcontracted staff) have signed a confidentiality agreement with the Com[any. This covers confidential data and personal data for which the Com[any is responsible. All confidentiality requirements are documented in a set of clauses in the agreement and in the internal regulations. If a specific project has specific confidentiality requirements, all involved parties (including employees) sign and adhere to these conditions.
11. The protection of the intellectual property of the Operator or the Authorized Person is ensured through access control procedures, confidentiality clauses, and contractual obligations. In cases where EDI employees have access to data subject to intellectual property rights and/or falling under GDPR, copying, reverse engineering, decompiling, and transferring actions on software, proprietary data, or personal data are prohibited, except where permission is explicitly granted by virtue of the contract and/or is necessary for its execution.
12. The Com[any's subcontractors have undertaken to accept second-party security audits to confirm compliance with its requirements in relation to the personal data for which it is responsible.

Technical Measures for the Protection of Employee Data

1. The Com[any uses cloud resources located in Europe for running applications and storing information and personal data. This type of infrastructure has the highest levels of physical security and cybersecurity on the server side.
2. Cloud resources have triple redundancy and run in high availability mode.
3. Laptops, other portable equipment, and terminals are protected by passwords, access restrictions, and encryption.
4. Connection to internal and external servers is only made via VPN or Remote Desktop, according to the requirements of the procedures and contracts.
5. All storage devices, including portable ones, are encrypted and password protected.
6. Clock synchronization is maintained by a cloud Time Server.
7. According to the asset inventory, all computers have real-time antivirus protection, with daily updates to Windows Defender.
8. Access to the physical archive is only permitted to authorized individuals. Access rights are reviewed annually in the Internal Audit.
9. All access rights, both computer and physical, are granted, modified, and suspended from management consoles by administrators in accordance with onboarding and offboarding procedures. These access rights reviews occur both at hiring or departure from the company and at entering or leaving a project.
10. Access to the internal or client infrastructure containing personal data is only permitted to authorized individuals and is done through VPN.

Transfers to Third-party Organizations and Countries

The company does not make transfers to third-party organizations and countries.

Communication

Data subjects can exercise their rights through notifications and requests sent in writing to the email address dataprotection@easydataintegration.net as a single point of contact. Any request should be documented in writing to minimize ambiguity and improve traceability.

Annexes

- Agreement for the processing of personal data with employees
- Agreement for the processing of personal data with customers and suppliers
- Register/Inventory of personal data