Information Security and Personal Data Protection Policy

Seargin Sp. z o.o.

Ul. Chrzanowskiego 11

80-278 Gdańsk, Poland

Contents

Information Security and Personal Data Protection Policy

Purpose of Policy and Outline

This policy constitutes a set of policies regulating various areas of information security and personal data protection within the organization. The objective of the Information Security and Personal Data Protection Policy is to ensure the protection of data, systems, and IT infrastructure against various threats, such as cyberattacks, data breaches, loss of information integrity, and risks associated with improper data management. The Information Security and Personal Data Protection Policy includes the following:

- Clean desk policy;
- Clean screen policy;
- Password policy for IT system users;
- Key and access control policy for rooms;
- Monitoring policy;
- Policy for granting authorizations to process personal data;
- Remote work policy;
- Policy to manage risks and conduct analysis and impact assessment;
- Internal and external audit policy;
- Cryptographic mechanism application policy;
- Backup policy;
- Policy for fulfilling information obligations and rights of data subjects;
- Authentication policy;
- Policy for concluding contracts with Customers and Suppliers;
- Incident and breach management policy;
- Data retention policy.

Main objectives of the Information Security and Personal Data Protection policy

1. **Data confidentiality protection:** Ensuring that only authorized persons have access to information, and that data is stored and processed in a way that protects its confidentiality.
2. **Maintaining data integrity:** Preventing unauthorized modification, deletion or destruction of data to maintain its accuracy and immutability.
3. **Ensuring data availability:** Guaranteeing that data is available to authorized users at the right time and place, regardless of possible disruptions or attacks.
4. **IT infrastructure protection:** Ensuring the security of computer systems, networks and devices, to prevent attacks and secure the infrastructure against potential threats.
5. **Compliance with regulations and standards:** Adjusting activities to applicable legal regulations and standards and standards regarding personal data protection and information security.
6. **User awareness and education:** Ensuring that employees, as well as persons performing work on the basis of titles other than an employment contract, are aware of the risks related to information security and have the appropriate knowledge and skills in the field of data protection.
7. **Incident response:** Developing policies for responding to information security incidents, including rapid identification, analysis, and elimination of threats and minimizing damage.
8. **Continuous improvement:** Continuously monitoring the IT environment, assessing risks, and implementing improvements and updates to adapt to changing threats and technologies.

Policy implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

Clean Desk Policy

Purpose of policy and outline

The purpose of the clean desk policy is to define rules that will prevent unauthorized access to data in the workplace- in particular, unauthorized persons gaining access to passwords, programs, applications or physical access to the computer and documents..

1. Employees are obliged to ensure that any documents or electronic media containing personal data or information that is confidential are not left in a publicly accessible place when:
    a. The employee has finished working at his/her workstation.
    b. The employee leaves his/her work station.
2. Electronic equipment including laptops, computers should:
    a. Be set in such a way that the screen is invisible to persons not authorized to process.
    b. Be blocked (screen saver set) when the workstation is left by the employee.
    c. Be completely switched off at the end of the work day.
3. In particular, it is forbidden to write down data such as identifiers, logins, passwords on cards that are hidden under the keyboard, phone flap, stuck to the monitor or left in any other way.
4. Keys to cabinets and drawers containing paper documents or data carriers cannot be stored or left in a place where persons who are not authorized to process personal data may be present.
5. Printed or scanned documents should be removed from the device immediately.
6. Documents intended for destruction should be immediately destroyed in a shredder.

Policy implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

Clean Screen Policy

Purpose of policy and outline

The purpose of the document is to ensure the protection of data confidentiality and minimize the risk of information leakage by controlling access to computer screens and applying measures to prevent unauthorized access.

1. Protection against disclosure of information:
    a. Recommendation to place monitors in places where it minimizes the possibility of potential disclosure of confidential company information to third parties.
    b. Using appropriate blinds, curtains or sunshades to limit access to monitors from outside.
2. Work Ergonomics:
    a. Requirement to set monitors at an appropriate height and distance from employees' eyes to ensure the privacy of information and minimize the risk of reading by unauthorized persons.
3. Appropriate Lighting:
    a. Providing even lighting in the workplace to minimize eye fatigue and prevent potential reading of information by unauthorized persons.
    b. Avoiding lighting conditions that are too bright or too dark, which can make it easier or harder to read information on the screen.
4. Login and lock screen:
    a. Requiring employees to secure their computers by locking their screens or logging out of the operating system when they leave their workstation. This helps prevent unauthorized individuals from accessing confidential data when the employee is away.

Policy implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

Password policy for IT system users

Purpose of policy and outline

The purpose of this policy is to introduce principles and unified standards specifying the conditions that should be met by passwords used by persons providing work/services to Seargin and the management of information that is the so-called secrets, i.e. access keys to services, services or hardware configurations.

User password recommendations

1. The user password for the IT system should consist of at least 12 characters, including at least 1 uppercase letter, 1 lowercase letter, 1 digit and 1 special character.
2. The organization uses Multi-factor authentication (MFA), which protects information media.
3. The password cannot be constructed using information that is predictable, including:
    a. They cannot contain information relating to the employee, e.g. his/her personal data,
    b. They should not contain predictable and typical dictionary words.
4. User passwords may not be made available to other employees or third parties.

Managing application “secrets”

1. The Administrator is obliged to properly secure data other than user passwords, including:
    a. Application API keys, which are used to communicate with internal or external applications.
    b. Access data to databases.
    c. Data used for cryptography.
    d. Access keys, which are the so-called secrets of an application or IT solution.
2. Access to access keys should be limited only to employees indicated by the data administrator.
3. The Information Systems Administrator ensures that the President of Management Board of the organization and persons appointed by the President of Management Board can obtain access to passwords, access keys and other secrets through an internally defined procedure.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

Key Policy and Access Control to Rooms

Purpose of policy and outline

The purpose of the Key Policy and Access Control to Rooms is to introduce an access control mechanism to enable the recording of employees' entries and exits from the data administrator's premises.

Requirements and recommendations

1. The data controller shall implement appropriate physical and technical protection measures for the premises where personal data are processed.
2. The Data Administrator, with the support of the Administration Department, keeps records of the issued physical and technical protection measures for access to the premises, including:
    a. Room keys.
    b. Magnetic cards.
3. Termination of the contract with the employee is tantamount to his/her obligation to return the means of access to the data controller's premises.
4. The administrator records the date of return of the transferred means of access to the administrator's premises.
5. The presence of unauthorized persons in the area of personal data processing is only permitted with the consent of the data controller or in the presence of a person authorized to process personal data.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

Monitoring Policy

Purpose of policy and outline

The monitoring policy defines the principles related to the use of monitoring techniques, which include monitoring of the telecommunications network and monitoring of e-mail, as well as other databases or telecommunications programs used in the organization.

General principles of using monitoring

1. Monitoring may only be used to ensure employee safety, protect property, maintain process continuity or maintain the confidentiality of information, the disclosure of which could expose the employer to damage.
2. Monitoring may not violate personal rights, including dignity, confidentiality of correspondence and freedom, as well as the rights of third parties.
3. Monitoring may be used in relation to the data controller's employees as well as subcontractors who use the data controller's infrastructure or equipment.
4. Information about the use of monitoring must be communicated no later than 2 weeks before the monitoring is launched in the customary manner, or before the employee is allowed to work.
5. It is strictly forbidden to use work email for private purposes, including redirecting work messages to private electronic accounts, media or disk spaces.
6. The data protection officer must be informed of the intention to introduce a new form of monitoring or a significant modification of the monitoring operation or infrastructure.
7. The introduction of a new form of monitoring requires the data controller to conduct a risk analysis and an impact assessment for data protection, unless there is an exemption from this obligation. The data protection officer will issue an opinion on the documentation submitted to him.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

Policy of granting authorizations to process personal data

Purpose of policy and outline

The purpose of this policy is to define the principles and criteria for granting authorizations to persons processing personal data within the organization, including supervision over the granted authorizations for processing. The policy ensures compliance with data protection regulations and minimizes the risk of privacy breaches.

Managing rights to process personal data

Appropriate management of data processing rights is a key element of our organization in the context of compliance with the provisions of the General Data Protection Regulation (GDPR) and ensuring the protection of personal data against unauthorized access and misuse. As part of our policy:

- Access to personal data is granted in accordance with the roles and responsibilities of employees in the organization, as well as partners and suppliers.
- We provide specific internal procedures for managing access to personal data, which include granting, modifying and removing access to personal data. These procedures are designed to effectively control access and prevent excessive access to data.
- The criteria for granting access take into account business needs and the principles of compliance with applicable regulations.
- The organization has implemented appropriate technical and organizational security measures to ensure the confidentiality, integrity and availability of personal data. Our procedures ensure that data is processed in accordance with applicable regulations and only by authorized persons.

Policy Implementation

1. The application of this policy begins on the date of its adoption by the authorized body.
2. This policy supersedes previous policies and procedures governing the area it addresses.
3. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, contractors, trainees, interns).
4. The Data Processing Authorization Manual applies to this policy.

Remote work policy

Purpose of policy and outline

The purpose of this document is to define the basic principles that are intended to raise awareness in connection with remote work. All employees, co-workers, trainees, interns (hereinafter referred to as employees) are required to comply with these provisions.

Requirements and recommendations

1. All policies and procedures established for work on the premises of the data controller also apply to remote work.
2. Employees are obliged to ensure that personal data is processed remotely with full confidentiality of the data processed by, among others:
    a. Selecting a safe place that will prevent unauthorized persons from viewing device screens to process personal data (e.g. working in public transport, hotels or other public places such as restaurants).
    b. Securing access to the official data held and preventing access to the data by third parties, including those living together with him, and against their unauthorized destruction or modification.
    c. Connecting to a secured home WiFi network. It is prohibited to use open WiFi networks, such as hotel WiFi, WiFi in shopping malls or hot spots in cafes.
    d. Regularly update your operating system and run a firewall.
3. In the event of loss or theft of equipment, documents or other information carriers, the incident must be reported immediately, on the day of the incident, to the direct superior, the Internal IT department, as well as the Compliance department and the Data Protection Inspector.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, contractors, trainees, interns).
3. This policy supersedes previous policies and procedures governing the area it addresses.
4. The Remote Work Regulations apply to this policy for employees.

Internal and external audit policy

Purpose of policy and outline

The purpose of this policy is to establish procedures related to conducting internal and external audits aimed at improving the personal data protection system and information security system within the organization. It applies to Senior Management, the Data Protection Officer, Team Leaders/Managers, and designated internal auditors within the organization.

Requirements and recommendations

1. Information security audits will be conducted no less than once a year, covering areas of IT infrastructure and personal data protection, encompassing all departments of the organization, unless specific departments are explicitly indicated as not requiring audits at this frequency.
2. During the audit, a review of all documentation related to information security and personal data protection will be conducted.
3. Audits are carried out following their approval by Senior Management.
4. The audit schedule is set in collaboration with Team Leaders/Managers typically up to one week before the audit begins, unless Senior Management agrees to a shorter timeframe.
5. In the event of a major incident or breach of information security or data protection, including suspected threats to information security, the IMS team, supported by the Data Protection Officer, may conduct an ad-hoc audit without the need for prior approval.
6. The rights of external auditors are defined in contracts.

Policy implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

Cryptographic Mechanisms Application Policy

Purpose of policy and outline

The purpose of this document is to introduce requirements regarding the use of cryptographic mechanisms to prevent unauthorized access to personal data by third parties. It applies to the President of the Management Board, Directors, Internal IT department (Information Systems Administrator) and all employees. The data controller must provide appropriate measures to ensure that appropriate cryptographic mechanisms are used throughout the organization.

Cryptographic mechanisms should include, among others:

1. Network connections between IT systems and web applications.
2. Memories in stationary and mobile devices.
3. Memories in portable memory devices such as USB sticks and portable drives.
4. Electronic correspondence, when possible.
5. Passwords saved in IT system databases.
6. Connecting users to the data administrator's services (VPN networks).
7. The Internal IT department ensures that all applications using SSL / TLS protocols have certificates issued by a known and trusted provider.
8. The Data Protection Inspector organizes an annual review of the application of this policy, which is carried out through the Internal IT department.
9. The Internal IT department introduces procedures for managing cryptographic keys.

Policy implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

Backup policy

Purpose of policy and outline

The purpose of this policy is to create standards for making backup copies and to indicate responsibility for the process related to making backup copies in the organization, in connection with ensuring business continuity and guaranteeing the protection of the rights of data subjects. Responsible for the process of making backup copies are the President of the Management Board, Directors, Internal IT department, employees when backup copies are decentralized and Subcontractors providing services to the data administrator.

Requirements and recommendations for electronic copies

Backups must be made at least once a week. Electronic backups must be made, especially for:

a. Relational and non-relational databases.
b. Programs that are necessary to read specific databases containing personal data.
c. System libraries and other IT system dependencies that are necessary to read specific databases containing personal data.
d. The data administrator is obliged to provide a procedure that will enable the removal of personal data also from backup copies in connection with the right to be forgotten resulting from the provisions of the General Data Protection Regulation as well as in connection with the data storage period (resulting from legal provisions and internal data retention policy).
e. The data administrator should conduct regular backup restoration tests to verify the correctness of their execution and the duration of the backup restoration process.
f. The data administrator should carry out regular tests of the infrastructure restoration procedure in case of its complete failure.

Including provisions regarding making backup copies

Provisions in contracts related to data processing should include appropriate guarantees related to the handling of backup copies in order to protect the personal data being processed and ensuring business continuity. Backup copies should be returned or deleted after the contract expires in accordance with the contractual provisions, unless the parties agree on separate procedures in the course of terminating the contract in writing or electronically using a qualified electronic signature.

Policy Implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

Policy for implementing information obligations and rights of data subjects

Purpose of policy and outline

The purpose of this policy is to define the principles of communication and information management provided for by the provisions on the protection of personal data, consisting in providing the data subject with information about the ongoing processing operations of his or her personal data and the purposes of such processing, as well as ensuring the implementation of the rights of persons whose personal data are processed, in accordance with art. 15-21 of the regulation about personal data protection.

Scope of the policy

This policy for the implementation of information obligations and rights of data subjects applies to all persons whose data are processed.

Rules for exercising the rights of data subjects

1. Any requests by persons regarding their rights specified in Art. 15-22 GDPR, are immediately forwarded to your inbox for processing rodo@seargin.com.
2. The request is implemented immediately, but no later than within one month of receiving the request. The response to requests, along with information about the actions taken, is carried out from the mailbox rodo@seargin.com.

Policy Implementation

1. The implementation of this policy begins upon its adoption by senior management.
2. This policy supersedes the previous policy governing the area it addresses.
3. The attached Request Processing Manual for Data Subject Requests applies to this policy.
4. The provisions of this policy are directed at all employees, as well as individuals performing work based on arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).

Authentication policy

Purpose of policy and outline

The purpose of this document is to introduce requirements for IT systems so that the authentication process guarantees an appropriate level of security. Applies to all employees.

1. The data controller ensures, as far as possible, that multi-factor authentication for IT systems is used, including, among others:
    a. Authentication using ID and password.
    b. Authentication with the additional use of one-time tokens.
    c. Authentication with the additional use of one-time SMS codes.
    d. Authentication with additional use of hardware authentication mechanisms, e.g. YubiKey, SmartCard.
2. Whenever possible and justified, the data administrator introduces mechanisms that enforce the use of multi-factor authentication on users of IT systems.
3. Multi-factor authentication mechanisms should also apply to server infrastructure.
4. Access control systems should also be used for particularly protected rooms.

Policy Implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

Policy for concluding contracts with customers and suppliers

Purpose of policy and outline

The purpose of introducing the contractual policy is to ensure consistency, compliance with the GDPR and efficiency in the process of concluding contracts for the processing of personal data between our organization and other entities. This policy aims to establish clear guidelines that will be used when negotiating, concluding, monitoring and managing contracts in our organization. By properly managing information security risk, standardizing processes and raising employee awareness, we want to minimize potential risks while optimizing the process.

1. In the case of concluding or terminating a contract with a Customer or Service Provider where there are doubts in the area of personal data protection, the person responsible for concluding this contract should inform the Compliance Department in order for it to analyze the contract from the point of view of personal data protection and information security.
2. The Compliance Department, with substantive support, analyzes contracts for compliance with applicable data protection regulations.
3. After analysis, the document is sent back to the person who submitted it for verification.
4. All contracts concluded within the organization are concluded via the Auteni platform.

Policy Implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

Risk Management Policy and Impact Assessment

Purpose of policy and outline

The purpose of this policy is to ensure compliance with applicable regulations and minimize the risk of security incidents and data breaches through appropriate risk management, risk analysis, and impact assessment.

Scope of the policy

The policy applies to all processes involving personal data processing and ICT system management within the organization, especially those that may pose a high risk to the rights and freedoms of individuals and to the continuity of the organization's operations.

Risk management

1. The IMS team is responsible for developing and implementing the risk management strategy within the organization.
2. Regular risk assessments related to ICT technologies are conducted, including the identification of critical functions, processes, and assets, as well as the analysis of potential threats and vulnerabilities.
3. As part of incident management, the IMS team is responsible for updating the Incident and Breach Management Policy to ensure effective response to events that require classification, reporting, and management.
4. Operational resilience tests and cybersecurity incident simulations are conducted to evaluate the effectiveness of security measures, identify security gaps, and assess the organization's preparedness for ICT-related incidents.
5. Development of business continuity and disaster recovery plans.
6. Personnel education to raise awareness of threats and responsibilities regarding organizational security.

Risk analysis

1. The IMS Team, with the support of the Data Protection Officer, conducts risk analyses related to personal data processing within their respective departments.
2. Risk assessments should include, among others:

   a. Information assets.

   b. Personal data processing processes.

   c. Service providers in relation to the delegation or potential delegation of personal data processing, where applicable.

   d. Potential threats associated with ICT infrastructure and their impact on the operational resilience of the organization.

e. Threats related to access management to systems and data, compliance with legal and industry regulations, financial risk management.

3. Risk analyses or their reviews must be conducted at least once a year.
4. The Data Protection Officer, in collaboration with the IMS Team, verifies the conducted risk analyses and their substantive accuracy regarding personal data.

Data protection Impact assessment

1. The Data Protection Officer is directly responsible for conducting data protection impact assessments and liaising with the data protection authority only when such an obligation arises from regulations.
2. A data protection impact assessment is conducted once for a personal data processing process and also in cases of changes to processing processes or new projects involving personal data processing.
3. Initiated projects may require a data protection impact assessment, but an initial evaluation of whether this will be necessary must be conducted by the IMS Team with the support of the Data Protection Officer.

Policy Implementation

1. This policy takes effect on the date of its adoption by the authorized body.
2. This policy replaces the previous policy concerning the regulated area it addresses.
3. The provisions of this policy are directed at all employees, as well as individuals performing work based on agreements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
4. This policy is subject to the Risk Assessment Manual and the Business Continuity Plan (BCP).

Incident and breach management policy

Purpose of policy and outline

The purpose of this policy is to establish principles and procedures for managing incidents and security breaches to: a. Ensure business continuity and the protection of data and systems in accordance with the NIS2 Directive (Network and Information Systems Directive 2); b. Minimize operational and cyber risks in compliance with the DORA (Digital Operational Resilience Act) requirements; c. Meet data protection requirements according to GDPR (General Data Protection Regulation). This policy also aims to ensure a prompt response to incidents, reduce their impact, and continually enhance the organization's security standards.

Scope of policy

The policy applies to all incidents related to: a. Information security, including personal data; b. Key services and the organization's critical infrastructure; c. Compliance with regulatory standards (NIS2, DORA, GDPR). The policy covers all employees, IT service providers, business partners, and entities processing data on behalf of the organization.

Key principles

1. Early Detection: Monitoring systems and business processes to identify potential threats.
2. Real-Time Response: Swift and coordinated actions to minimize the impact of incidents.
3. Compliance: Incident reporting in line with DORA, NIS2, and GDPR requirements.
4. Personal Data Security: Safeguarding personal data in compliance with Articles 33 and 34 of GDPR.

Incident reporting

Any event that could impact business continuity, critical infrastructure security, operational incidents, cybersecurity incidents, or data protection breaches must be promptly reported via email to:

- rodo@seargin.com – for events involving personal data protection breaches
- incidents@seargin.com – for events involving business continuity, critical infrastructure security, operational incidents, and cybersecurity incidents.

Policy implementation

1. This policy takes effect upon adoption by senior management.
2. This policy supersedes any previous policies governing the regulated area it addresses.
3. The provisions of this policy apply to all employees, as well as individuals performing work based on agreements other than an employment contract (e.g., B2B contractors, contractors, trainees, interns).
4. This policy is subject to the Business Continuity Plan (BCP), GDPR Incident and Breach Management Manual, NIS2 Incident Management Manual, and DORA Incident Management Manual.

Data retention policy

Purpose of policy and outline

The purpose of this policy is to define the deadlines for deleting personal data from information media in order to implement the principle of "storage limitation" in accordance with Art. 5 section 1 letter e GDPR. The data retention policy applies to all employees processing personal data and to all information media containing personal data, in particular:

a. personal data in programs, applications and systems;
b. paper documentation,
c. e-mail messages,
d. recordings,
e. data in control and access systems.

Requirements and recommendations

The Personal Data Protection Inspector is responsible for periodically assessing the time during which personal data is processed and, with the support of the Compliance Department, reviewing the purposes of personal data processing in terms of their storage period.

Personal data retention periods

The basis for establishing retention dates is:

- Contract- The retention period for personal data processed under the contract is counted from the date of termination of the relationship, i.e. from the termination or execution of the contract.
- Consent- The data retention period is counted from the date of withdrawal of this consent by the person who granted it.
- Legitimate interest of the administrator- data processing is necessary for the purposes of the legitimate interests pursued by the administrator or a third party, and there are no situations in which these interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring data protection personal data.
- Legal provision (legal obligation).

When establishing retention periods, particular consideration has been taken into account:

- Legal obligations of the Administrator in terms of storing specific Personal Data or documents containing Personal Data, arising from applicable legal provisions;
- The necessity of processing Personal Data for purposes related to determining or pursuing claims and defending against such claims and the related limitation periods for claims resulting from the relevant legal provisions;

- Retention periods specified in the RCP may change due to changes in applicable legal provisions affecting the retention period or due to the Administrator's decision, of which persons employed in the Administrator's organization and cooperating with it will be informed;
- To comply with a legal obligation requiring processing under Union law or the law of a Member State to which the Controller is subject.

Data retention period

Personal data should be deleted in accordance with the deadlines indicated in the data retention table below:

Process name	Legal record	Retention period
Realization of rights and employer's obligations	Art. 7 section 2 of the Act of January 10, 2018 amending certain acts in connection with the shortening of the storage period of employee files and their electronification (Journal of Laws of 2018, item 357): - employed on January 1, 2019, 50 years [Art. . 51u(1) of the Act of 14 July 1983 on the national archival resources and archives (Journal of Laws of 2018, item 217, consolidated text)] 50 years [Art. 125a(4) of the Act of 17 December 1998 on pensions and annuities from the Social Insurance Fund. Exception: submission of the report referred to in Art. 7 section 3 of the Act of January 10, 2018 amending certain acts (...) - employed after January 1, 2019. For the period of employment and then 10 years from the end of the calendar year, in which the employment relationship has expired or been terminated (Article 94(9b) of the Labor Code).	50 or 10 years. Employee penalties are removed upon request or after a period of impeccable work.
Data processing within the Company's Social Benefits Fund	Art. 8 section 1 letter C and D of the Act on the Company Social Benefits Fund.	The employer processes personal data referred to in section 1a, for the period necessary to grant the reduced service and benefits, subsidies from the Fund and determine their amount, as well as for the period necessary to pursue rights or claims. The employer reviews the personal data referred to in section 1a, at least once a calendar year in order to determine the necessity of their further storage. The employer deletes personal data whose further storage is unnecessary to achieve the purpose specified in section 1a and 1c.
Using additional rights for employees, e.g. the Benefit system	Art. 70 of the Tax Ordinance §1. The tax liability expires after 5 years, counting from the end of the calendar year in which the tax payment deadline expired.	5 years from the end of the calendar year when the contract was terminated.
Video monitoring of employees	Art. 222 § 3 of the Labor Code.	A period not exceeding 3 months from the date of recording.
Use of employee images	Consent pursuant to Art. 22a and 22a of the Labor Code.	Consent pursuant to Art. 22a and 22a of the Labor Code.

Email monitoring	Art. 6 section 1 letter f) GDPR in connection with joke. 223 of the Labor Code.	Determined by the employer.
Mandatory and optional training	Art. 7 section 2 of the Act of January 10, 2018 amending certain acts in connection with the shortening of the storage period of employee files and their electronicization (Journal of Laws of 2018, item 357): - employed on January 1, 2019, 50 years [Art. . 51u(1) of the Act of 14 July 1983 on national archival resources and archives (Journal of Laws of 2018, item 217, consolidated text)] 50 years [Art. 125a(4) of the Act of 17 December 1998 on pensions and annuities from the Social Insurance Fund. Exception: submission of the report referred to in Art. 7 section 3 of the Act of January 10, 2018 amending certain acts (...) - employed after January 1, 2019. For the period of employment and then 10 years from the end of the calendar year in which the employment relationship expired or was terminated (Article 94(9b) of the Labor Code).	50 or 10 years Employee penalties upon request or after a period of impeccable work.
Registering employees for social security	Art. 41c and Art. 41f of the Act on the social security system.	10 years
Maintaining accounting and tax documentation.	Accounting Act.	5 years from the end of the calendar year in which the tax payment deadline expired.
Agreements with contractors	Civil Code	10 years from the end of cooperation.
Umowy z klientami	Civil Code	10 years from the end of cooperation.
Documentation related to occupational health and safety	art. 234 § 31 of the Labor Code	10 years

Annex No. 4 of the Data Retention Manual applies to this policy.

Related documents

Registers

- Register of data processing activities
- Register of categories of processing activities
- Incident register
- Register of authorizations to process personal data of internal employees
- Register of authorizations for the Partner
- Register of the implementation of GDPR rights

Attachments

- Manual for granting authorizations to process data
- Risk estimation manual
- Business Continuity Plan (BCP)
- GDPR incident and breach management manual
- NIS2 incident and breach management manual
- DORA incident and breach management manual
- Manual for transferring requests from entities for execution
- Remote working regulations

Other

- Personal data breach reporting form Data breach notification form

List of changes

Document author	Document version	Date updated	Valid from	Notes
Piotr Siemieniak	1	19.01.2018	01.02.2018	Basic document.
Piotr Siemieniak	2	25.05.2018	25.05.2018	Monitoring policy added.
Piotr Siemieniak	3	20.09.2021	20.09.2021	Updated information assets policy and information classification.
Piotr Siemieniak	4	15.11.2021	01.12.2021	Expanding the communication policy.
Michał Zajdowicz Klaudia Krajewska	5	16.11.2022	21.11.2022	Policies updated, Data Retention Policy and related documents added.
Klaudia Krajewska	6	20.02.2023	06.04.2023	Remote work policy update.

Document author	Document version	Date updated	Valid from	Notes
Monika Kotowicz Michał Zajdowicz Klaudia Kacala Mikołaj Gumowski	7	21.11.2023	01.01.2024	Delimitation of responsibilities between the Compliance, Legal, Internal IT and IOD departments. Separation of the policies "Implementation of rights of data subjects" and "Communication of information and implementation of information obligations". Changing security (passwords, VPN, Bitcloker) in the Internal IT area.
Monika Kotowicz Klaudia Kacala Szymon Słupczyński	8	25.04.2024	06.05.2024	Removing the list of changes in the document and adding a clean screen policy. Exclusion from the Information Security and Personal Data Protection Policy of provisions relating to procedures that constitute attachments as an integral part of the Policy.
Monika Kotowicz Klaudia Kacała	9	01.07.2024	01.08.2024	Unification of nomenclature, supplementation of the risk assessment procedure, restoration of the list of changes in the document.
Klaudia Kacała Aleksandra Siemaszko	10	03.10.2024	15.11.2024	Change of annexes from procedures to manuals Update the document Policy for conducting risk analysis and impact assessment - alignment under NIS2 and DORA Introduction of NIS2 incident and breach management manual and DORA incident and breach management manual Introduction of the Business Continuity Plan (BCP) as an appendix.

Gdańsk, 14.11.2024

Jakub Wojewski

President of Management Board

KARTA PODPISÓW

poświadczenie złożenia podpisów i pieczęci elektronicznych

Certyfikat dla dokumentu o Autenti ID: fb51ec6b-eb86-4aab-badd-948fc96616be
utworzonego: 2024-11-15 09:01 (GMT+01:00)

Dokument przekazany do podpisu przez SEARGIN SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ iso@seargin.com, został zabezpieczony pieczęcią elektroniczną Autenti przed wprowadzeniem nieautoryzowanych zmian.

2024-11-15 09:01 (GMT+01:00)

Jakub Wojewski
jakub.wojewski@seargin.com

SEARGIN SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
NIP: 5833165868 | Prezes Zarządu

Podpis elektroniczny zabezpieczony pieczęcią Autenti

Uwierzytelnienie: e-mail

Powód: Podpisanie dokumentu

Adres IP: 87.204.192.62

2024-11-15 11:27 (GMT+01:00)

Autentyczność oraz integralność podpisanego dokumentu przed wprowadzeniem nieautoryzowanych zmian została zabezpieczona pieczęcią elektroniczną Autenti.

2024-11-15 11:28 (GMT+01:00)

Niniejszy dokument stanowi poświadczenie wykonania usługi zaufania, w tym złożenia podpisów elektronicznych, zgodnie z zasadami opisanymi w Polityce.

Osoby podpisujące dokument złożyły podpisy elektroniczne zgodnie z zasadami opisanymi w Polityce Usług Zaufania Autenti dla podpisów elektronicznych Autenti oraz obsługi podpisywania dokumentów (dostępnej na: https://autenti.com/pl/regulaminy) oraz oświadczyły, że znają i akceptują treść podpisywanego dokumentu a także potwierdziły poprawność i prawdziwość danych służących do złożenia podpisu elektronicznego.

W ramach składania podpisów elektronicznych przeprowadzono uwierzytelnienie podpisujących.

Usługa została wykonana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Rozporządzenie eIDAS).

Karta podpisów stanowi poświadczenie Autenti w zakresie realizacji poszczególnych usług zaufania, zgodnie z zasadami ich świadczenia oraz definicjami zawartymi w Polityce.