SecureBlock

Data Protection Policy

Secure Block d.o.o.

January 18th 2026

Contents

Revision history:

Version	***Revision Date***	***Author***	***Description***
1.0	*November 28th 2022*	*Luka Šikić* 	*Initial version*
1.1	*May 4th 2023*	*Luka Šikić*	*Updates to Privacy by Design*
1.2	*November 28th 2024*	*Mirna Novak*	*Updates to Procedures*
1.3	*January 18th 2026*	*Mirna Novak*	*Updates to Chapter 17s*

1. Introduction

This Data Protection Policy Document applies to the processing of personal data in manual and electronic records kept by Secure Block d.o.o. in connection with its human resources function as described below. It also covers the Secure Block d.o.o. response to any data breach and other rights under the General Data Protection Regulation.
This policy applies to the personal data of:

- Current, past and prospective employees
- Customers (B2C)
- Users of its websites
- Clients (B2B)
- Other stakeholders

These are referred to in this policy as relevant individuals.
The purpose of this policy is to set out the relevant legislation and to describe the steps Secure Block d.o.o. is taking to ensure that it complies with it.
This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Secure Block d.o.o. systems.

2. The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a standout amongst the most noteworthy parts of enactments influencing the way that Secure Block d.o.o. handles data. Under GDPR, enforcement approaches including fines are set if a data breach is deemed to have happened due to non-compliance with GDPR, which is intended to secure the individual information of nationals of the European Union. It is the intention of Secure Block d.o.o. to guarantee the consistency with the GDPR and other important enactment in a clear, verifiable, and consistent manner.

3. GDPR Fundamental Concepts

The most important concepts from the GDPR regulation that are consistent within Secure Block d.o.o. and apply properly for this policy are the following:
"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.
"Controller" is the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“Special categories of personal data” is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).
“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.
In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

4. Principles related to processing of personal data

As stated in the GDPR regulation, there are 7 principles involving personal data and how companies should treat these aspects.
These are as follows, as per Chapter II, Article 5.1.

1) Personal data shall be:
    a) processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
    b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89., not be considered to be incompatible with the initial purposes (“purpose limitation”);
    c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
    d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay (“accuracy”);
    e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);
    f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).
2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).

Secure Block d.o.o. complies with these principles by having a clearly defined set of rules and policies regarding gathering and processing of personal data. All personal data is kept and appropriately updated in the Data Asset Inventory table, alongside the necessary type,

source, location, purpose, lawful bases, and storage period defined for each data item. Furthermore, defined Operational Security Procedures support and provide the specific guidelines for all teams involved including IT Support, Customer Support or Line of Business (LOB).

5. Employee Responsibilities

Any staff member of Secure Block d.o.o. who is involved in the collection, storage or processing of personal data has responsibilities under the legislation.
Any staff member involved in the processing/storing of personal data should make sure to:

- obtain and process personal data fairly
- keep such data only for explicit and lawful purposes
- disclose such data only in ways compatible with these purposes
- keep such data safe and secure
- keep such data accurate, complete, and up to date
- ensure that such data is adequate, relevant, and not excessive
- retain such data for no longer than is necessary for the explicit purpose

Any data access requests received should be forwarded immediately to the Compliance Management, Information Management, or relevant management personnel.

6. Rights of Individuals

The data subject has rights under the GDPR.
As stated in the GDPR regulation, these are as follows, as per Chapter III, Articles 12-23.

1) The right to be informed.
2) The right of access.
3) The right to rectification.
4) The right to erasure.
5) The right to restrict processing.
6) The right to data portability.
7) The right to object.
8) Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Secure Block d.o.o. that allow the required action to be taken within the timeframes stated in the GDPR, as shown below:

Data Subject Request	**Timeframe**
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	Without undue delay
The right to erasure	Without undue delay

The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Undefined

7. Consent

Unless it is necessary for a reason allowable according to the GDPR, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about the usage of personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.
If personal data is not obtained directly from the data subject, then this information must be provided within a reasonable period after the data is obtained, which is no more than within one month.

8. Procedures

Secure Block d.o.o. has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access by enforcing the following:

- Appointing an employee with specific responsibilities for:
  - the processing and controlling of data
  - the comprehensive reviewing and auditing of its data protection systems and procedures
  - overviewing the effectiveness and integrity of all the data that must be protected
- Setting clear lines of responsibility and accountability for the role
- Providing information to its employees on their data protection rights, how it uses their personal data, and how it protects it; the information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- Providing its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- Being able to account for all personal data it holds, where it comes from, who it is shared with and who it might be shared with
- Carrying out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security; the procedure includes an assessment of the impact of both use and potential misuse of personal data in and by Secure Block d.o.o.

- Recognizing the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions; Secure Block d.o.o. understands that consent must be freely given, specific, informed and unambiguous; Secure Block d.o.o. will seek consent on a specific and individual basis where appropriate and full information will be given regarding the activities about which consent is sought; relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- Establishing appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches; Secure Block d.o.o. is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the relevant Data Protection Authority (DPA), and is aware of the possible consequences
- Being aware of the implications international transfer of personal data internationally

9. Access to Data

Relevant individuals have a right to be informed whether Secure Block d.o.o. processes personal data relating to them and to access the data that the Secure Block d.o.o. holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- A subject access request should be made to contact@secureblock.io or support@pentestpad.com
- Secure Block d.o.o. will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- Secure Block d.o.o. will respond to a request without delay; access to data will be provided, subject to legally permitted exemptions, within one month; timeframe may be extended by additional two months where requests are complex or numerous

Relevant individuals must inform Secure Block d.o.o. immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. Secure Block d.o.o. will take immediate steps to rectify the information.
For further information on making a subject access request, employees can refer to the Secure Block d.o.o. Data Subject Request document.

10. Privacy by Design

Secure Block d.o.o. has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.
The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data

- Definition of controls that are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation shall be considered where applicable and appropriate.

11. Data Disclosures

Secure Block d.o.o. may be required to disclose certain data/information. The circumstances leading to such disclosures include:

- employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- Statutory Sick leave payment purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- smooth operation of any employee insurance policies or pension plans

These kinds of disclosures will only be made when strictly necessary with a justified purpose.

12. Data Security

Secure Block d.o.o. adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the Information Security Policy document.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- under no circumstances share their personal account credentials
- use computer screen locking or blanking to ensure that personal data is not left on screen when not in use

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless there is a justifiable business need. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left unsupervised

Failure to follow Secure Block d.o.o. rules on data security may be dealt with via the Secure Block d.o.o. disciplinary procedure. Appropriate sanctions may include dismissal with or without notice dependent on the severity of the breach.

13. Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.
Intra-group international data transfers must be subject to legally binding agreements, such as Data Processing Agreements (DPA) which provide enforceable rights for data subjects.

14. Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale.
Based on these criteria, it is not required for the Data Protection Officer to be appointed at Secure Block d.o.o.
Nevertheless, due care and due diligence related to GDPR compliance is performed by formally appointed personnel, without assuming the DPO role.

15. Breach notification

It is a Secure Block d.o.o. policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the internal GDPR responsible personnel will inform the relevant Data Protection Authority (DPA) within 72 hours. This will be managed in accordance with the Information Security Incident Management Policy which sets out the overall process of handling information security incidents.

16. Addressing compliance to the GDPR

The following actions are undertaken to ensure that Secure Block d.o.o. complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- Responsible employee is appointed with specific responsibility for data protection in the organisation
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details

- Purposes of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
- Personal data retention schedules
- Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management review process of the information security management system.

17. Obligations of Secure Block d.o.o.

Secure Block d.o.o. stores and processes data of relevant individuals. Personal data is stored in personnel files and Client files (B2B) within the HR systems of Secure Block d.o.o., or within its internal cloud infrastructure.
The following types of data may be held by Secure Block d.o.o., as appropriate, on current, past and prospective employees:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- Personal Identification numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details

The following types of data may be held by Secure Block d.o.o., as appropriate, on Customers (B2C) or users of its websites:

- name, address, phone numbers
- email address
- phone numbers
- billing/delivery address details
- Web Browser Cookies

The following types of data may be held by Secure Block d.o.o., as appropriate, on Clients (B2B):

- name, address, phone numbers
- email address
- phone numbers
- conduct issues such as letters of concern, disciplinary proceedings
- internal performance information
- training details
- Anonymized PostHog information on website movements for bug fixes purposes

Full list along with further details is provided in the Data Asset Inventory table.

Relevant individuals should refer to the Secure Block d.o.o. publicly accessible Privacy Policy for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.
According to the code of practice for protection of personally identifiable information (PII), Secure Block d.o.o. also provides the following policy guidance:

- Relevant individuals are provided with means to meet their obligations under law in activities such as accessing, amending and erasing PII
- Gathered PII is only used for Relevant individuals processing purposes, and not for further purposes of Secure Block d.o.o. such as data selling or user profiling
- Relevant individual is informed if Secure Block d.o.o. is required by law to disclose any of their data, unless Secure Block d.o.o. is prohibited from doing so
- Details of disclosures are recorded
- Secure Block d.o.o. informs relevant individuals about using subcontractors to process their PII
- Secure Block d.o.o. will alert relevant individuals if their PII is subject to unauthorised access