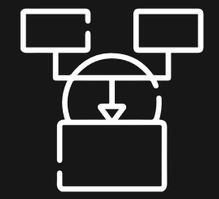
Personal data protection policy at Vitrintec Sp. z o.o.

VITRINTEC®
wall solutions

Introduction

Vitrintec Sp. z o.o. acts as the Data Controller, whereas personal data protection activities are performed by the Chairperson of the Management Board, Tomasz Rybka. He is obliged to take all measures necessary to prevent risks related to the processing of personal data.
The Personal Data Protection Policy is a document describing the principles of personal data protection applied by the Controller in order to meet the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in relation to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC and the Act of 10 May 2018 on personal data protection (Journal of Laws 2018, item 1000).

The purpose of this Personal Data Protection Policy is to fulfil the objectives of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 EC (General Data Protection Regulation, hereinafter referred to as GDPR). It constitutes a set of rules, principles and regulations concerning the protection of personal data by the Data Controller.



CHAPTER 1

General provisions

§ 1

For the purposes of this document, the following definitions shall apply:

1. 1. Policy - the Personal Data Protection Policy at Vitrintec Sp. z o.o.,
2. 2. Personal Data - any information relating to an identified or identifiable natural person. An identifiable person is an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more characteristic features of his/her physical, physiological, mental, economic, cultural or social characteristics.
3. 3. Data set - a structured set of personal data which are accessible according to specific criteria, regardless of whether the set is centralised, decentralised or dispersed on a functional or geographical basis.
4. 4. Controller – a natural or legal person, public authority, organisational unit or other entity that alone or jointly with others determines the purposes and means of the processing of personal data.
5. 5. Processor - a natural or legal person, public authority, organisational unit or other entity that processes personal data on behalf of the Controller;
6. 6. Risk - an indicator of a condition or event that may lead to damage. It is proportional to the likelihood of that event occurring and to the extent of damage it may cause.
7. 7. Processing– any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, e.g. 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.
8. 8. Recipient - a natural or legal person, public authority, organisational unit or other entity to whom personal data is disclosed. Public authorities that may obtain personal data in the course of proceedings in accordance with EU or Member State regulations are not considered recipients.
9. 9. Data Subject Consent - a freely given, specific, informed and unambiguous demonstration of will by which the data subject, by means of a written statement or a clear confirmatory action, consents to the processing of personal data concerning him/her.
10. 10. Breach – a security incident that may lead to an accidental or unlawful damage, loss, modification, unauthorized access to personal data transferred, stored or otherwise processed.

§ 2

1. The purpose of the Policy is to:

   a) ensure the protection of personal data processed at Vitrintec Sp. z o.o.

   b) establish uniform rules of conduct for the processing of personal data,

   c) implement organisational and technical measures that ensure the processing of personal data in compliance with the law, in particular with the GDPR, and to be able to demonstrate this compliance.

2. The specific objectives of the Policy are:

   a) ensuring that the rights of personal data subjects are exercised,

   b) determining the duties and responsibilities of persons obliged to per form the tasks set out in the Policy,

   c) ensuring the performance of data protection impact assessments,

   d) managing and mitigating personal data protection violations,

   e) introducing employees to the changes in the regulations concerning personal data.

3. Scope of application of the Policy

   a) The Policy sets out the manner in which personal data is processed and the procedures related to the processing of personal data are managed to ensure adequate protection of such data. The Controller or Co-controller is the President of the Management Board.

   b) The Policy also defines the manner in which personal data is pro cessed and the management of processes related to the processing of per sonal data to ensure adequate protection of such data,

   c) The Policy defines the duties and responsibilities of the persons obliged to implement the tasks related to the processes concerned.

   d) The Policy applies to the processing of the personal data regardless of:

   1) the method of processing (fully automated, partially automated or other than automated),

   2) the form or format of the processing (paper, electronic or other),

   3) the channels of flow of personal data,

   4) the IT tools used to process personal data (systems, applications, pro grams),

   5) the purpose of the processing,

   6) the source of the personal data,

   7) the categories of personal data,

   8) The Policy shall be applied by all persons who, on the request of the Data Controller, participate in the processing of personal data.

CHAPTER 2

Data inventory.

Principles of personal data processing.

Accountability. Information obligation.

Agreements and contacts

with external parties.

§ 3

1. Personal data requiring protection is listed in the Annex to this Policy (Annex 1 - List of personal data sets).
2. The list includes sets with an identified potential risk of infringement of the rights or freedoms of individuals.
3. Each data set is described in a way that enables a review of the risk.
4. The description of the sets includes such information as:
    a) the name of the data set,
    b) description of the purposes of the processing,
    c) nature, scope, context, personal data documented,
    d) recipients,
    e) functional description of the processing operations,
    f) the assets used to process the personal data,
    g) information on the obligation to conduct an impact assessment for the data set,
    h) the category of data subjects,
    i) data of the controller - the person responsible for the collected data,
    j) planned deletion dates,
    k) the legal basis of the processing.

§ 4

1. The controller and the processor shall ensure that personal data are processed in accordance with the following rules:

    a) lawful and fair and transparent for the data subject (lawfulness, fairness and transparency),

    b) collected for specified, explicit and legitimate purposes (purpose limitation),

    c) adequate, relevant and not excessive in relation to the purposes for which they are processed (data minimisation),

    d) accurate and, where necessary, kept up to date (accuracy),

    e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the processing, with the exceptions indicated in the Regulation (storage limitation),

    f) in a manner which ensures adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of technical and organisational measures appropriate to the risks and the category of data protected, and in particular protected against their disclosure to or access by an unauthorised person (integrity and confidentiality),

    g) The so-called information obligation - the right of access to data, data portability, rectification, erasure, restriction of processing and objection - has been exercised with regard to the persons whose data are processed.

2. The controller keeps a register of processing activities. The register is at the same time a list of personal data sets processed by the Controller (Annex 1).
3. The Processor shall maintain a register of categories of processing activities.

§ 5

1. All employees of Vitrintec Sp. z o.o., irrespective of their basis of employment and persons carrying out activities on the basis of civil law contracts, who process personal data as part of their duties, are obliged to apply the principles set out by this document.
2. Any person with access to personal data processed at Vitrintec Sp. z o.o. is required to read this document.

§ 6

1. The controller/processor is responsible for granting and cancelling authorisations to process personal data in paper files, IT systems.
2. The processor and any person acting under the authorisation of the controller or processor and having access to personal data shall process them only on instructed by the controller, unless required by law.
3. Authorisations are granted to data sets at the request of supervisors (heads/department heads). Heads of organisational units define the scope of authorisation to process personal data.
4. Authorisations define the scope of data operations.
5. Authorisations should be kept in the personnel files of employees (eventually in the files of the relevant committees), should be made available only to authorised persons and should be updated in case of changes in the scope of duties.
6. Authorisations may exceptionally be given in the form of orders, e.g. authorisation to conduct inspections, audits, perform official activities.
7. The controller shall keep a register of authorised persons in order to control the proper access to the data. The register constitutes an Annex to this Policy (Annex No. 2 - Specimen register of authorised persons). The records are kept in electronic form.

§ 7

8. Authorisation to process personal data in the IT system is granted at the request of superiors (heads/directors of departments) of persons who are obliged to process the data. In appropriate cases, such a request may be made by employees. The request for a resource related to personal data is made by e-mail to the IT specialist within the organisation, and the supervisor is also informed (e-mail CC).
8. Heads of organisational units of departments shall specify the IT systems to which employees of their departments have access and the scope of their rights.
8. The authorisation referred to in para. 1 shall be cancelled upon termination of the processing of personal data by the person to whom the authorisation was granted or upon termination of employment.

§ 8

1. The controller, when obtaining personal data from the data subject, is obliged to provide him/her with the following information:

   a) identity and contact details,

   b) the purposes of the data processing and the legal basis for the processing

   c) if the processing of personal data is related to the exercise of legitimate interests pursued by the controller or by a third party - the legitimate interests must be indicated,

   d) information on the recipients or categories of recipients of personal data

   e) where applicable, information about the intention to transfer the data to a third country or an international organisation,

   f) the period for which the personal data will be stored and, where this is not possible, the criteria for determining that period,

   g) information on the right to request from the controller access to, rectification, erasure or restriction of processing of personal data concerning the data subject, or the right to object to the processing as well as the right to data portability,

   h) information about the right to withdraw consent at any time without affecting the legitimacy of the data processed on the basis of consent prior to its withdrawal (this rule applies to the processing of data on the basis of consent expressed for one or more purposes and to the processing of special categories of data on the basis of the data subject's consent),

   i) information on the right to lodge a complaint to the supervisory body

   j) information whether the provision of the data is a statutory or contractual obligation or a condition for entering into a contract and whether the data subject is obliged to provide the data and the possible consequences of failing to do so,

   k) information on automated decision-making.

2. Where the controller obtains personal data from a different source than the data subject, the Controller is obliged to provide the data subject with all the information listed in para. 1, and additionally: disclose information on the source of personal data.

3. The information referred to in para. 2 shall be provided by the controller within a reasonable time after the data have been obtained, at the latest within one month having regard to the specific circumstances of the personal data processing. Where personal data are to be used for communication with the data subject, the controller shall provide the data at the latest at the first such communication. If it is planned to disclose personal data to another recipient at the latest at the first disclosure.

§ 9

1. Personal data may only be used for the purposes for which they were, are or will be collected and processed for no longer than is necessary to achieve the above mentioned purposes. Personal data may be stored for longer periods if they will be processed exclusively for archiving purposes in the public interest, for scientific or historical purposes or for statistical purposes.

2. Personal data should be kept in a form which does not allow the identification of the data subject.

3. The data subject shall have the right to request from the controller the rectification of data concerning him/her which are inaccurate.

4. The data subject shall have the right to request from the controller the immediate erasure of personal data concerning him/her, and the controller shall be obliged to erase the data without undue delay if one of the prerequisites occurs:

   a) the personal data are no longer necessary for the purposes for which they were collected,

   b) the data subject has withdrawn the consent on which the processing is based and there is no other legal basis for the processing,

   c) the data subject raises an objection pursuant to law and there are no overriding legitimate interests for the processing,

   d) the personal data has been unlawfully processed,

   e) the personal data must be erased in order to comply with a legal obligation,

   f) the personal data were collected in relation to the offering of information society services.

5. The data subject has the right to request the restriction of processing in the following cases:

   a) the data subject contests the accuracy of the data,

   b) the processing is unlawful, and the data subject objects to the erasure of the data,

   c) The controller no longer needs the personal data for the purposes of the processing, but the data are needed by the data subject to establish, assert or defend a claim,

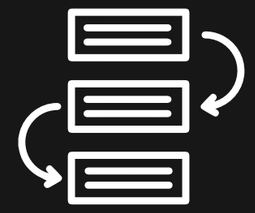
   d) The data subject has objected to the processing.

6. The data subject shall have the right to receive in a structured, commonly used machine-readable format the personal data concerning him or her which he or she has provided to the controller, and shall have the right to transfer such personal data to another controller without interference from the controller to whom the personal data have been provided.

7. The data subject has the right not to be subject to a decision which is based solely on automated processing, including profiling, and which produces legal effects concerning him or her or which similarly significantly affects him or her.

§ 10

1. If the processing is to be conducted on behalf of the controller, it shall use only the services of such processors that provide sufficient guarantees for the implementation of appropriate technical and organisational measures so that the processing meets the requirements of this Regulation and protects the rights of the data subjects.
2. Data are processed by a processor on the basis of a contract or other legal instrument, binding the processor and the controller, specifying the object and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects, the obligations and rights of the controller.
3. When entering into agreements with external companies affecting the operation of key elements of the information security management system, it is recommended to conclude an entrustment agreement.



CHAPTER 3

Processing of personal data security risks.

Incident handling procedure.

§ 11

The Policy defines a set of vulnerabilities and incidents that threaten the security of personal data and describes how to manage them. Its purpose is to minimise the consequences of security incidents and reduce the risk of threats and incidents occurring in the future.

1. Each employee of the company is obliged to notify his or her direct superior immediately, no later than within 24 hours, if a vulnerability is identified or an incident occurs. If the incident concerns a digital data leak, the IT department must also be informed.
2. Typical personal data security vulnerabilities include in particular:

   a. inadequate physical security of premises, equipment and documents,

   b. inadequate protection of IT hardware and software against leakage, theft and loss of personal data,

   c. non-compliance with personal data protection principles by employees (e.g. non-application of the clean desk/screen principle, password protection, not locking rooms, cabinets, desks).

3. Typical personal data security incidents include in particular:

   a. external random events (facility/room fire, flooding, loss of power, loss of communications),

   b. internal random events (malfunctions of the server, computers, hard disks, software, mistakes made by IT staff, users, data loss/loss,

   c. deliberate incidents (hacking into the IT system or premises, theft of data or equipment, information leakage, disclosure of data to unauthorised persons, deliberate destruction of documents or data, operation of viruses or other malicious software).

4. If an incident is identified, the controller (in the case of digital data, involving the IT department) investigates in the course of which it

   a. determines the scope and causes of the incident and its consequences,

   b. initiates possible disciplinary actions,

   c. acts to restore the organisation's operations after the incident has occurred,

   d. recommend preventive (precautionary) actions aimed at eliminating similar incidents in the future, or at reducing the losses when they occur.

5. The controller shall document the above-mentioned all personal data protection violations, including the circumstances of the personal data protection violation, its consequences and remedial actions taken (Annex No. 3 - Notification of personal data protection violation),
6. It is forbidden to cause incidents intentionally or unintentionally by persons authorised to process data.
7. In the case of a personal data breach resulting in a risk of infringement of the rights or freedoms of natural persons, the controller shall without undue delay - if possible, not later than 72 hours after the breach has been noticed - notify it to the supervisory authority.
8. In the event of an incident, the controller shall notify the data subjects of the incident.

CHAPTER 4

Data protection regulations,
key policy.

§ 12

1. The Regulation determines the basic obligations of employees, co-workers, employees of third parties having access to personal data processed by the controller, users of IT systems with access to personal data processed by the controller to observe the principles of personal data protection in compliance with the regulations.
2. After reading the principles of personal data protection, persons are obliged to confirm their knowledge thereof and declare their application thereof (Annex No. 5 - Declaration on keeping personal data obtained at work confidential).

CHAPTER 5

Training/audit

§ 13

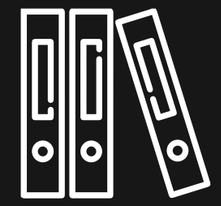
1. Each user, before getting access to the processing of personal data, is obliged to familiarise with the regulations in this area and learn about the resulting tasks and responsibilities.
2. All users are subject to periodic internal training.
3. The personal data controller shall be responsible for conducting the training.
4. If internal training on the principles of personal data protection is conducted, it is advisable to document it..
5. After the training on personal data protection principles, the participants are obliged to confirm their knowledge of these principles and declare their adherence.
6. According to Article 32 of the GDPR, the controller should regularly test, measure and evaluate the effectiveness of technical and organisational measures to ensure secure data processing.

CHAPTER 6

Organisational and technical
measures to protect personal data

§ 14

1. In accordance with Article 32 of the GDPR, the controller should ensure the ability to quickly restore the availability of and access to personal data. In the event of a physical or technical incident.
2. Procedures for restoring the availability of and access to personal data have been developed as an annex (Annex 10 - Business Continuity Plan).



CHAPTER 7

List of premises where documents containing personal data are processed at Vitrintec Sp. z o.o.

§ 15

The list of premises owned by Vitrintec Sp. z o.o. where personal data are processed, including sensitive premises, is attached to this Policy: Annex 4 - List of premises.

VITRINTEC®
wall solutions

The Data Protection Policy of Vitrintec Sp. z o.o. was adopted on 1 July 2024.