creo concept®

PERFECT WALL

Personal Data Protection Policy at CreoConcept Sp. z o.o. Sp. k.

creo concept®

PERFECT WALL

Dokumentacja zdjęciowa nie może być rozpowszechniana ani wykorzystywana do jakichkolwiek celów przez osoby trzecie.

Introduction

CreoConcept Sp. z o.o. Sp. k. is a Personal Data Controller, and personal data protection activities are performed by the President of the Management Board, Tomasz Rybka. He is obliged to take all possible 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 to meet the requirements of the Regulation of the European Parliament and of the Council (EU) 2016/679 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, and the Act of 10 May 2018 on the Protection of Personal Data (Dz. U. /Journal of Laws/ of 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 the GDPR). It constitutes a set of requirements, rules and regulations relating to the protection of personal data at the Personal Data Controller.

Chapter I
General provisions

§ 1

For the purposes of this document, the following definitions are introduced:

1. Policy – Personal Data Protection Policy at CreoConcept Sp. z o.o. Sp. k.,
2. Personal data - any information relating to an identified or identifiable natural person. A data subject shall be regarded as any person whose identity can be determined directly or indirectly, e.g. by reference to an identification number or to a factor defining physical, physiological, mental, economic, cultural or social characteristics.
3. Personal Data Set – an ordered set of Personal Data available according to specific criteria, regardless of whether the set is centralised, decentralised or distributed functionally or geographically.
4. Controller – natural or legal person, public authority, organisational unit or other entity which individually or jointly with others determines the purposes and means of the processing of personal data.
5. Processor - a natural or legal person, public authority, organisational unit or other entity that processes Personal Data on behalf of the Controller;
6. Risk – an indicator of a condition or event that may lead to losses. It is proportional to the probability of occurrence of this event and to the amount of losses it may cause.
7. Processing – operation or set of operations performed on personal data or personal data sets in an automated or non-automated way, such as: collecting, saving, preserving, organising, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, distributing or otherwise sharing, matching or combining, limiting, deleting or destroying.
8. Recipient - a natural or legal person, public authority, organisational unit or other entity to which personal data is disclosed, regardless of whether it is a third party. Public bodies that may obtain personal data as part of an ongoing proceeding in accordance with EU law or the law of a Member State are not considered recipients.
9. Consent of the data subject – means a voluntary, specific, conscious and unambiguous representation of the will, to which the data subject, in the form of a declaration or a clear confirmation action, authorises the processing of their Personal Data.
10. Personal Data Breach (incident) – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to Personal Data transmitted, stored or otherwise processed.

§ 2

1. The Policy serves to:

a) ensure the protection of personal data processed at CreoConcept Sp. z o.o. Sp. k.,

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 accordance with the law, in particular with the GDPR, and the possibility of demonstrating this compliance.

2. The specific objectives of the Policy include:

a) ensuring the implementation of the rights of data subjects,

b) defining the duties and responsibilities of persons obliged to carry out the tasks, as defined in the Policy,

c) ensuring that a data protection impact assessment is carried out,

d) managing and mitigating data protection violations,

e) method of communicating changes in Personal Data regulations to the employees.

3. Scope of Policy application

a) The Policy sets out how personal data is processed and how processes related to the processing of personal data are managed to ensure adequate protection of such data for which the controller or co-controller is the President of the Management Board of the company,

b) The Policy also specifies how personal data are processed and how processes related to the processing of personal data are managed to ensure adequate protection of such data,

c) The Policy defines the duties and responsibilities of persons required to perform tasks related to the processes in question,

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

1. the method of processing (fully automated, partially automated or other than automated),
2. the form of processing (paper, electronic or other),
3. the channels of personal data flow,
4. IT tools for processing personal data (systems, applications, programmes),
5. the purpose of processing,
6. the source of personal data,
7. the category of personal data,
8. The Policy shall be applied by all persons who, on instructions from the Controller, participate in the processing of personal data.

Chapter II

Data inventory. Principles of personal data processing. Liability. Information obligation. Agreements and contact with external parties.

§ 3

1. Personal data requiring protection are listed in the appendix to this Policy (Appendix No. 1 – List of personal data sets).
2. The list includes sets with an identified potential risk of violation of the rights or freedoms of individuals.
3. Each set is described in such a way as to enable a risk analysis.
4. The description of the sets includes the following information:
   a) the name of the set,
   b) description of the processing purposes,
   c) nature, scope, context, documented personal data,
   d) recipients,
   e) functional description of processing operations,
   f) assets used to process personal data,
   g) information on the need to conduct a set impact assessment,
   h) category of data subjects,
   i) data of the controller, i.e. the person responsible for the collected data,
   j) scheduled data deletion dates,
   k) legal basis for processing.

§ 4

1. The Controller and the Processor shall ensure that personal data are:

   a) processed lawfully, fairly and in a transparent manner for the data subject (lawfulness, fairness and transparency),

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

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

   d) accurate and updated as necessary (accuracy),

   e) stored in a form enabling the identification of data subjects for a period no longer than necessary for their processing, with the exceptions indicated in the regulation (storage limitation),

   f) processed in a way that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using technical and organisational measures appropriate to the threats and categories of data protected, and in particular secured against making them available to persons unauthorised or acquired by an unauthorised person (integrity and confidentiality),

   g) The so-called "information obligation" – the right of data access, portability, rectification, deletion, restriction of processing and objection – has been exercised against data subjects.

2. The Controller shall keep a record of processing activities. The record is at the same time a list of personal data sets processed by the Controller (Appendix 1).

3. The processor shall maintain a register of categories of processing activities.

§ 5

1. All CreoConcept Sp. z o.o. Sp. k. employees, irrespective of their basis of employment, and any persons carrying out activities under civil law contracts who process personal data as part of their professional duties shall comply with the principles set out herein.

2. Every person who has access to personal data processed at CreoConcept Sp. z o.o. Sp. k. shall read and understand this document.

§ 6

1. The Controller/Processor shall be responsible for granting and revoking authorisations to process personal data in paper data sets and IT systems.

2. The Processor and any person acting under the authority of the Controller or the Processor and who has access to personal data shall only process personal data on instructions from the Controller unless they are legally required to do so.

3. Data set access authorisations shall be granted at the request of supervisors (department heads/directors). The scope of personal data processing shall be defined by the heads of organisational units.

4. Authorisations shall specify the scope of data operations.

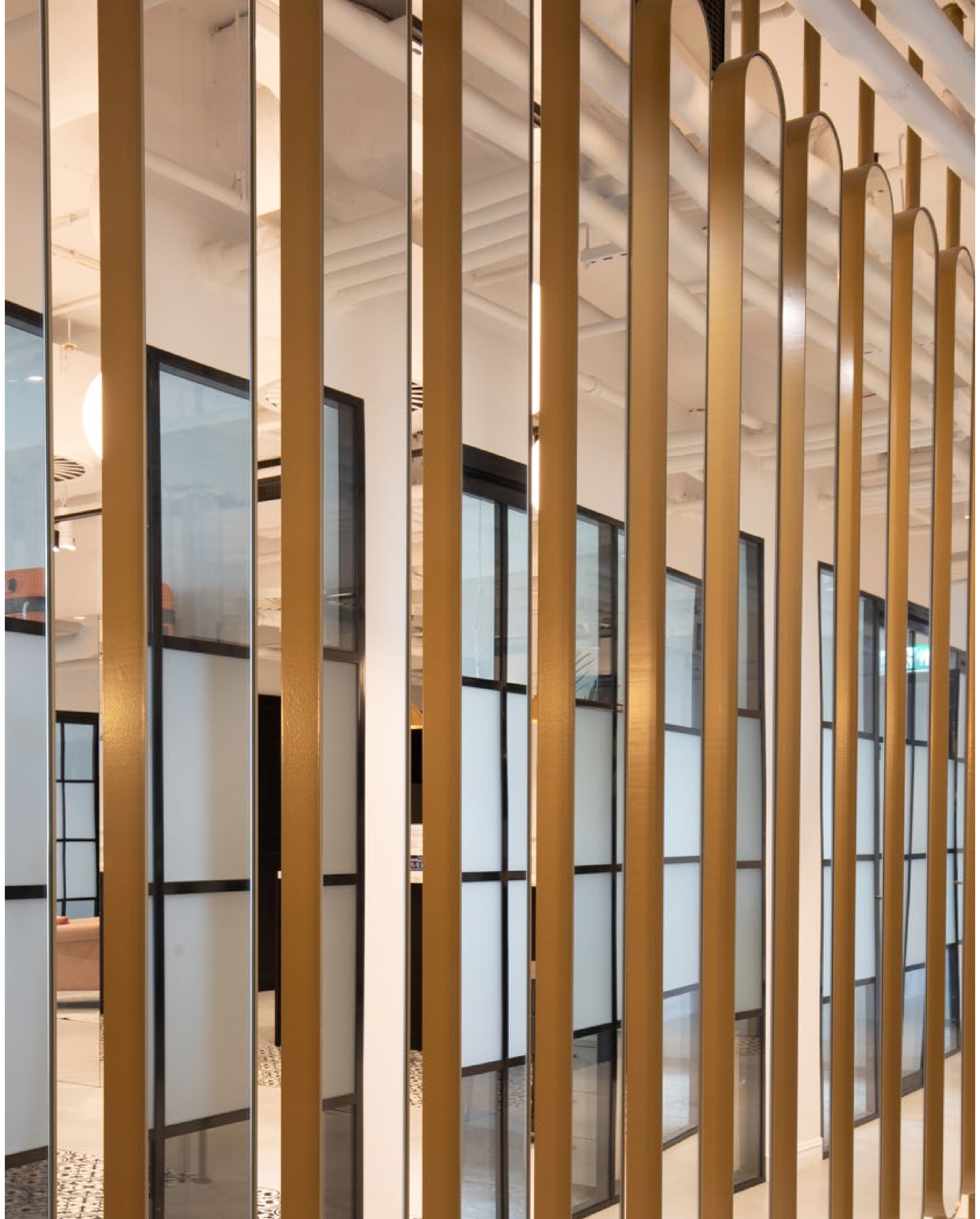
5. Authorisations shall be kept in the staff files (or in the files of the relevant committees), shall only be made available to authorised persons and be updated upon each change in the scope of responsibilities.

6. In exceptional cases, authorisations may be given in the form of orders, e.g. authorisation to carry out inspections, audits, or perform official duties.

7. The Data Controller shall keep a register of authorised persons to monitor proper data access by authorised individuals. The register constitutes an appendix to this Policy (Appendix 2 - Specimen register of authorised persons). The register shall be kept electronically.

§ 7

1. Authorisations to process personal data in the IT system shall be granted at the request of the superiors (department heads/directors) of the persons who are to process the data. Employees may request such authorisations where the situation requires it. Requests for access to personal data resources shall be made by email to the organisation's IT specialist with a Carbon Copy to the supervisor (CC e-mail).
2. Heads of departmental organisational units shall determine the IT systems to which their departmental staff have access and their areas of responsibility.
3. The authorisation referred to in item 1 shall be revoked from the cessation of the processing of personal data by the authorisation holder or the termination of the holder's employment.



§ 8

1. When obtaining personal data from a data subject, the Controller shall be obliged to provide the data subject with the following information:
   a) Controller's identity and contact details,
   b) purposes and legal basis of Personal Data Processing;
   c) where personal data processing is related to the pursuit of a legitimate interest by the Controller or by a third party, such legitimate interest shall be indicated,
   d) information on personal data recipients or recipient categories,
   e) where applicable, information about the intention to transfer the data to a third country or an international organisation,
   f) personal data storage period, and where this is impossible, the criteria for determining such period,
   g) information about the right to request from the Controller the access to Personal Data relating to the data subject, its rectification, removal or limitation of processing or the right to object to the processing, as well as the right to transfer personal data,
   h) information on the right to withdraw consent at any time without affecting the lawfulness of the processing carried out based on consent before its withdrawal (this applies to the processing of data based on consent for one or more purposes and to the processing of special categories of data based on the data subject's consent),
   i) information on the right to lodge a complaint with a supervisory authority,
   j) information on whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data,
   k) information on automated decision-making.
2. Where the Controller obtains personal data from a source other than the data subject, the Controller shall provide the data subject with all the information listed in item 1 and additionally provide information on the source of personal data.
3. The Controller shall provide the information referred to in item 2 within a reasonable time after data acquisition and, in any case, no later than within one month, taking into account the specific circumstances of the processing of the personal data. Where personal data are to be used for communicating with the data subject, the Controller shall transmit the data during the first such communication at the latest. If disclosure to another recipient is planned, this shall be done no later than the first data 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 purposes of processing. Personal data may be retained longer if it is processed exclusively for archival purposes in the public interest or for scientific, historical or statistical purposes.
2. Personal data shall be kept in a form that does not enable the identification of the data subjects.
3. The data subjects shall have the right to request from the Controller the rectification of any incorrect data subject-related data.
4. The data subjects shall have the right to request from the Controller the immediate deletion of personal data concerning them, and the Controller shall be obliged to delete such data without undue delay where any of the following prerequisites apply:
   a) the personal data are no longer necessary for the purposes for which they were collected,
   b) the data subject has withdrawn consent on which the processing is based, and there are no other legal grounds for the processing,
   c) the data subject has legally objected to the processing, and no overriding legitimate interests exist to warrant further processing,
   d) the personal data have been processed unlawfully,
   e) the personal data has to be erased for compliance with a legal obligation,
   f) the personal data have been collected in connection with offering information society services,
5. The data subject shall have the right to demand from the Controller restriction of processing in the following cases:
   a) The data subject disputes data accuracy,
   b) The processing is unlawful and the data subject objects to data deletion,
   c) The Controller no longer needs the personal data for the purposes of processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims,
   d) The data subject has objected to the processing.
6. The data subject shall have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.
7. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or affects them in a similarly significant way.

§ 10

1. Where the processing is to be carried out on behalf of the controller, the controller shall use only processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this regulation and ensure the protection of the rights of the data subjects.
2. Processing by a processor shall be carried out based on an agreement or other legal instrument, binding the processor and the Controller, setting out the subject matter 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, an entrustment agreement is recommended.

Chapter III
Dealing with personal data security incidents.

Instruction on incident handling.

§ 11

The procedure identifies a catalogue of vulnerabilities and incidents that threaten the security of personal data and describes how to respond to them. Its purpose is to minimise the effects of security incidents and to reduce the risk of threats and incidents occurring in the future.

1. Every employee of the company shall notify their immediate supervisor immediately, within 24 hours at the latest, if a vulnerability is identified or an incident occurs. If the incident involves the leakage of digital data, 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 equipment, and software against leakage, theft and loss of personal data,
   c) non-compliance of employees with the principles of personal data protection (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 incidents (fire of the facility/room, flooding, loss of power, loss of communications),
   b) internal random incidents (failures of the server, computers, hard disks, software, mistakes of IT staff, users, deletion/loss of data,
   c) intentional incidents (intrusion into the IT system or premises, theft of data or equipment, leakage of information, disclosure of data to unauthorised persons, intentional destruction of documents or data, operation of viruses and other malicious software).
4. If an incident is identified, the Controller (in the case of digital data, involving the IT department) shall conduct an investigation, during which it shall:
   a) determine the scope and causes of the incident and its possible consequences,
   b) initiate possible disciplinary action,
   c) act to restore the organisation's operations following the incident,
   d) recommend preventive (precautionary) actions to eliminate similar incidents in the future, or to reduce losses when they occur.
5. The Controller shall document the above-mentioned breaches of personal data protection, including the circumstances of the personal data protection breach, its consequences and remedial actions taken (Appendix 3 - Personal data breach report),

6. It shall be prohibited to knowingly or unintentionally cause incidents by persons authorised to process data.
7. In the event 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 is identified – report it to a supervisory authority.
8. In the event of an incident, the Controller shall notify the data subjects of the incident.

Chapter IV **Data protection regulations, key policy.**

§ 12

1. The Regulations specify the basic duties in respect of observing the principles of personal data protection in accordance with the regulations for employees, co-workers, employees of third parties having access to personal data processed by the Controller, and users of IT systems with access to personal data processed by the Controller.
2. After reading the personal data protection principles, the persons are obliged to confirm their knowledge of these principles and declare that they will apply them (Appendix 5 - Declaration on keeping the personal data obtained during the work in secrecy).

Chapter V
Training / audit

§ 13

1. Each user, before being allowed to process personal data, shall read the regulations concerning this matter and learn about the tasks and responsibilities arising therefrom.
2. All users shall be subject to periodic internal training.
3. The Controller shall be responsible for conducting training.
4. If internal training on the principles of personal data protection is carried out, it is advisable to document that this training has taken place.
5. After the training on the principles of personal data protection, the participants are obliged to confirm their knowledge of these principles and declare their application.
6. Under Art. 32 of the GDPR, the Controller should regularly test, measure and evaluate the effectiveness of the technical and organisational measures to ensure the security of the processing.

Chapter VI
Organisational and technical measures to safeguard personal data

§ 14

1. Under Art. 32 of the GDPR, the Controller shall 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 drafted as an appendix (Appendix 10 - Business Continuity Plan).

Chapter VII
List of rooms where documents containing personal data are processed at CreoConcept Sp. z o.o. Sp. k.

§ 15

The list of rooms belonging to CreoConcept Sp. z o.o. Sp. k. in which operations on personal data are performed, including the particularly protected rooms, is enclosed with this policy as Appendix 4 - List of rooms.

Appendix 1 – The list of Controller's personal data set
Appendix 2 - Specimen register of authorised persons
Appendix 3 - Notification of a personal data breach
Appendix 4 - List of rooms
Appendix 5 - Declaration of confidentiality of personal data obtained in the course of work

creo concept®

PERFECT WALL

Personal Data Protection Policy at CreoConcept Sp. z o.o. Sp. k. was adopted on December 8, 2023.

Publications of CreoConcept Sp. z o.o. Sp. k.

THINK CREO