# Centro-Chem Sp. z o.o. Sp.k.

# PERSONAL DATA PROTECTION POLICY

**at Centro-Chem Sp. z o.o. Sp.k.**
**with its registered office in Turka**

**Turka 2025**

## Spis treści

## Introduction

Centro-Chem limited liability company limited partnership in Turka, Turka 141B, 20-258 Lublin, entered into the Register of Entrepreneurs under KRS number: 0000822639, NIP: 7132339236, REGON: 43093238600000, hereinafter referred to as "Centro-Chem sp. z o.o. sp.k." or the "Company", respects the privacy of individuals whose data it processes and exercises the highest diligence to ensure that such data is processed in accordance with the law and international best practice principles. The Company makes particular efforts to protect the privacy and information entrusted to it, carefully selecting and applying appropriate technical, IT, and organisational measures ensuring the protection of processed data, in particular safeguarding the data from being shared with unauthorised persons, disclosed, lost, destroyed, unlawfully modified, or processed in violation of applicable legal provisions.

This Personal Data Protection Policy, hereinafter the "Policy", has been prepared to demonstrate that personal data is processed and secured in accordance with the legal requirements concerning the rules of processing and securing data at Centro-Chem sp. z o.o. sp.k., hereinafter the "Controller", including in particular the provisions 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 – GDPR)[1], the Act of 10 May 2018 on the Protection of Personal Data[2], as well as other legal acts applicable to the processing of personal data and privacy protection.

To ensure the protection of the privacy of data subjects, Centro-Chem sp. z o.o. sp.k. applies strict internal and external safeguards. As the Controller of personal data, Centro-Chem sp. z o.o. sp.k. maintains constant oversight over the data processing procedures and restricts access to data to the greatest extent possible, granting appropriate authorisations only when necessary for the proper processing of personal data.

[1] 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) (OJ L 119, p. 1)
[2] Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781)

## Chapter I
## General Provisions

### § 1

1. Whenever the following terms are used in this Policy without further specification, they shall mean:
    1) **Controller (ADO)** – this shall be understood as the personal data controller, i.e., Centro-Chem limited liability company limited partnership, Turka 141B, 20-258 Lublin, entered into the Register of Entrepreneurs under KRS number: 0000822639, NIP: 7132339236, REGON: 43093238600000;
    2) **Anonymisation of personal data** – this shall be understood as the removal of characteristics from personal data that allow the identification of the natural persons to whom the data relates;
    3) **Personal data database** – this shall be understood as a set of thematically related, organised data stored, for example, in the internal or external memory of a computer. A database consists of elements with a defined structure – records or objects in which personal data is stored;
    4) **Information security** – this shall be understood as ensuring the confidentiality, integrity, and availability of processed personal data;
    5) **Personal data** – this shall be understood as any information relating to an identified or identifiable natural person;
    6) **Special categories of personal data** – this shall be understood as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning that person's health, sexuality, or sexual orientation. Annex No. 2 constitutes a template to this Policy;
    7) **Regular personal data** – this shall be understood as all personal data that does not constitute special categories of personal data. Annex No. 1 constitutes a template to this Policy;
    8) **Availability** – this shall be understood as the guarantee that access to personal data is granted only to authorised individuals;
    9) **Password** – this shall be understood as a sequence of 9 characters (letters, digits, and other special characters) known only to the person authorised to work in the IT system. A password must contain at least: one uppercase letter, one lowercase letter, one digit, and one special character;

10) **User identifier** – this shall be understood as a sequence of letters, numbers, or other special characters that uniquely identifies a person authorised to process data in an IT system;
11) **Incident** – this shall be understood as a personal data protection breach;
12) **Data integrity** – this shall be understood as the property ensuring that personal data has not been altered or destroyed in an unauthorised manner (by unauthorised persons);
13) **Login (identifier)** – this shall be understood as an alphanumeric sequence unique to each user accessing IT resources processed and stored on a server or within a networked IT system;
14) **Data Protection Officer (DPO)** – this shall be understood as the person formally appointed by the Controller, responsible for: informing the Controller, Processor, and Employees who process personal data of their duties under applicable data protection regulations and advising them in this regard; monitoring compliance with data protection laws and with the Controller's or Processor's data protection policies, including assigning responsibilities, raising awareness, training personnel involved in processing activities, and conducting related audits; providing guidance on data protection impact assessments and monitoring their implementation;
15) **Personal data breach** – this shall be understood as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data transmitted, stored, or otherwise processed;
16) **Processing area** – this shall be understood as rooms or parts of office rooms forming an area in which the Company or its employees process personal data;
17) **Restriction of processing** – this shall be understood as marking stored personal data in order to limit their future processing;
18) **Supervisory authority** – this shall be understood as the President of the Personal Data Protection Office (PUODO), or, if applicable, the competent supervisory authority for personal data designated by another Member State of the European Union;
19) **Unauthorised person** – this shall be understood as a person who does not hold an authorisation granted by the Personal Data Controller to process personal data;
20) **Confidentiality** – this shall be understood as the property ensuring that data is not disclosed;
21) **Data subject** – this shall be understood as a natural person whose personal data is processed by the Controller;
22) **Processor** – this shall be understood as a natural or legal person, public authority, unit, or other entity that processes personal data on behalf of the Controller;
23) **Data confidentiality** – this shall be understood as the property ensuring that data is not made available to unauthorised entities;

24) **Policy** – this shall be understood as this Personal Data Protection Policy, which includes, in particular, the set of technical and organisational measures for the protection of personal data introduced, implemented, and applied at Centro-Chem sp. z o.o. sp.k., necessary to ensure the confidentiality, integrity, and accountability of processed data as described in this document;
25) **Information Security Policy for IT Systems** – this shall be understood as the Information Security Policy for IT Systems applicable at Centro-Chem sp. z o.o. sp.k.;
26) **Employee** – this shall be understood as a natural person employed by the Controller under an employment contract;
27) **Data processing operation** – this shall be understood as a set of activities involving the processing of personal data;
28) **Profiling** – this shall be understood as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements;
29) **Data processing** – this shall be understood as any operation performed on personal data, such as collection, recording, storage, organisation, modification, disclosure, and erasure, whether in traditional form or within IT systems;
30) **Record of processing activities** – this shall be understood as a document that shows, in particular, which processes within Centro-Chem sp. z o.o. sp.k. involve personal data, for what purpose, to whom the data relates, and how it is secured. This document must be made available upon any request by the supervisory authority (PUODO);
31) **Accountability** – this shall be understood as the property ensuring that the actions of an entity can be uniquely attributed to that entity.
32) **Regulation** – this shall be understood as 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 – "GDPR");
33) **IT network** – this shall be understood as a structure consisting of servers, workstations, and network equipment connected by transmission media for the purpose of data exchange or resource sharing;
34) **Workstation** – this shall be understood as a desktop or portable computer forming part of an IT system, enabling system Users to access personal data stored within the system;
35) **IT system** – this shall be understood as a set of cooperating devices, programs, information processing procedures, and software tools used for data processing;

36) **Traditional system** – this shall be understood as a set of organisational procedures, mechanical information processing methods, equipment, and fixed assets used to process personal data in paper form;
37) **Data erasure** – this shall be understood as the destruction of personal data or such modification of the data that makes it impossible to determine the identity of the person to whom the data relates (data anonymisation);
38) **Act** – this shall be understood as the Act of 10 May 2018 on the Protection of Personal Data;
39) **Authentication** – this shall be understood as an action intended to verify the declared identity of an entity;
40) **User** – this shall be understood as a person authorised by the Controller to process personal data;
41) **Joint controllership** – this shall be understood as a situation in which at least two controllers jointly determine the purposes and means of personal data processing;
42) **Associate/Collaborator** – this shall be understood as a natural person providing services to the Controller under a civil law contract (e.g., contract of mandate, contract for specific work);
43) **Data security in an IT system** – this shall be understood as the implementation and operation of appropriate technical and organisational measures ensuring the protection of processed personal data, adequate to the risks and categories of data under protection, aimed in particular at securing the data against unauthorised disclosure, acquisition by an unauthorised person, alteration, loss, damage, or destruction;
44) **Personal data set** – this shall be understood as any structured set of personal data accessible according to specific criteria, regardless of its distribution or division;
45) **Event** – this shall be understood as information or a circumstance giving rise to a suspicion of a personal data protection breach, on the basis of which the risk of violating rights and freedoms is assessed. If no threat to rights and freedoms is identified, the event does not constitute a breach;
46) **Consent of the data subject** – this shall be understood as a declaration of will whereby the person expresses consent to the processing of their personal data; consent cannot be presumed or implied from a declaration of will of a different content.

2. This Policy applies to all employees of Centro-Chem sp. z o.o. sp.k., including interns, volunteers, trainees, suppliers, and entities cooperating on the basis of civil law contracts, who have any contact with protected personal data.
3. The Policy applies to all Personal Data processed at Centro-Chem sp. z o.o. sp.k., regardless of the form of processing (traditional processing, record collections, IT systems) and regardless of whether the data is or may be processed in personal data sets.

4. The Policy is stored in electronic form and in paper form at the Controller's registered office.
5. An electronic version of this Policy, identical in content to the written version, is made available to Processors and Users in order to familiarise them with the rules for processing and securing Personal Data used within the enterprise operated by the Controller.
6. For the effective implementation of the Policy, the Data Controller ensures:
    1) technical measures and organisational solutions appropriate to the risks and categories of protected data;
    2) control and supervision over the processing of personal data;
    3) monitoring of the applied protection measures.
7. Monitoring by the Data Controller of the implemented protection measures includes, among others: user activities, breaches of data access rules, ensuring file integrity, and protection against external and internal attacks.
8. The Data Controller ensures that all activities related to the processing and securing of personal data comply with this Policy and with the applicable legal provisions.
9. In the case of cooperation with a third party involving the processing of personal data on behalf of the Controller, the Company ensures that such a third party commits to providing an appropriate level of personal data protection, taking into account the provisions of this Policy.
10. In the case of cooperation with a third party involving the processing of personal data by the Controller on behalf of that third party, the Company concludes a data processing agreement and ensures compliance with its requirements by all persons involved in such cooperation.
11. Through appropriate technical and organisational measures, the Controller ensures the ability to demonstrate compliance of personal data processing with the GDPR and other personal data protection regulations (“accountability”).
12. When appointing a Data Protection Officer (DPO), the Controller ensures that the DPO reports directly to the Management Board of the Controller and avoids any conflict of interest between the DPO and the Company.
13. The implementation of this Policy aims to ensure GDPR compliance of all personal data processing activities carried out by the Controller, regardless of the form (electronic or paper) in which the processing occurs.

**§ 2.**

**Objectives, assumptions, and scope of the Personal Data Protection Policy**

1. The Policy constitutes a set of rules applicable to the processing of personal data at Centro-chem sp. z o.o. sp.k.
2. The Policy consists of:
    1) a description of the personal data protection rules applicable to the Controller;

2) annexes specifying and supplementing this Policy.

3. The objectives of the Policy are:
    1) to ensure an appropriate level of security of personal data at Centro-chem sp. z o.o. sp.k. by implementing an appropriate system protecting such data against internal and external threats;
    2) to raise the awareness of Centro-chem sp. z o.o. sp.k. employees regarding the importance of personal data security.
4. For the implementation and execution of this Policy, the Controller ensures:
    1) technical measures and organisational solutions appropriate to the risks and categories of Data under protection;
    2) control and supervision over the processing of Personal Data;
    3) monitoring of the applied protection measures.
5. Personal data protection at the Controller is based on the following assumptions:
    1) **Lawfulness** – the Controller takes care of privacy protection and processes data in accordance with the law;
    2) **Security** – the Controller makes every effort to ensure an appropriate level of data security;
    3) **Rights of data subjects** – the Controller enables individuals whose data it processes to exercise their rights and ensures that these rights are respected;
    4) **Accountability** – the Controller documents how it fulfils its personal data protection obligations so that it can demonstrate compliance with the GDPR at any time.
6. The Controller processes personal data in accordance with the following principles:
    1) **Lawfulness** – personal data is processed based on a specific legal basis and in compliance with the law;
    2) **Fairness** – personal data is processed fairly and ethically;
    3) **Transparency** – personal data is processed in a manner that is transparent to the data subject;
    4) **Data minimisation** – personal data is processed only to the extent necessary for the intended purposes;
    5) **Adequacy** – the processing of personal data is proportionate to the Controller's needs;
    6) **Storage limitation** – data is stored by the Controller for no longer than necessary for the purposes for which it is processed;
    7) **Accuracy** – personal data is processed with attention to its correctness;
    8) **Timeliness** – personal data is processed for the necessary and appropriate duration;
    9) **Integrity and confidentiality** – the Controller ensures appropriate security of personal data processing.

7. The principles established by this Policy apply to all personal data sets administered by the Controller, in particular to:
    1) all existing, currently implemented, or future IT and paper-based systems in which personal data subject to protection is or will be processed;
    2) personal data processed by the Controller both when it acts as the controller of such data and when it processes data entrusted to it under data processing agreements pursuant to Article 28 GDPR;
    3) all information carriers—e.g., paper, magnetic, optical media, etc.—on which personal data subject to protection is or will be stored;
    4) all locations — buildings and rooms in which personal data subject to protection is or will be processed;
    5) all employees within the meaning of the Labour Code, consultants, interns, and other persons who have access to personal data subject to protection.

## Chapter II

## Organisation of Personal Data Processing

### § 3.

1. The entity responsible for the processing of personal data is the Controller, who delegates duties to the Data Protection Officer (if appointed) and to its employees. The Controller bears legal responsibility for fulfilling its obligations in connection with the processing of personal data by itself or on its behalf. The primary obligation of the Controller is to ensure that processing is carried out in accordance with the GDPR and to be able to demonstrate this. For this purpose, the Controller must implement appropriate and effective technical and organisational measures:
    1) they must ensure the highest known and achievable level of protection at the time of processing;
    2) this is not a one-time activity—such measures must be reviewed and updated whenever necessary;
    3) the Controller carries this out taking into account the nature, scope, context, and purposes of processing, as well as the risk of violating the rights or freedoms of natural persons, considering the likelihood and severity of the threat;
    4) these measures include the implementation of a data protection policy by the Controller.
2. Under the GDPR, the Controller is obligated to:
    1) identify the legal basis for lawful processing of personal data;
    2) secure processed personal data against disclosure to unauthorised persons and against acquisition by an unauthorised individual;

3) process data in accordance with GDPR requirements;
4) protect data against alteration, loss, damage, or destruction.

3. These obligations should be fulfilled through:
   1) preparing documentation;
   2) keeping a register of persons authorised to process personal data — Annex No. 3 to this Policy — including interns, volunteers, trainees, and students processing data within the Company;
   3) monitoring the activities performed on each data set;
   4) ensuring technical security measures.
4. Regarding the information obligation, the data controller:
   1) communicates with data subjects (natural persons) and provides them with information in a concise, transparent, intelligible, and easily accessible form;
   2) acilitates the exercise of data subjects' rights;
   3) provides data subjects with information free of charge, including upon their request; the deadline for providing such information is one month, which may be extended to two months in complex cases;
   4) verifies the identity of persons submitting requests for information.
5. Regarding the rights of the data subject:
   1) the Controller confirms whether personal data relating to a given natural person is being processed and, if so, provides the information required under the Regulation;
   2) facilitates the data subject's exercise of their rights under Articles 15–22 GDPR;
   3) informs the data subject about the actions taken in relation to their requests based on Articles 15–22 GDPR;
   4) justifies any refusal to comply with a data subject's request and informs them of their right to lodge a complaint;
   5) enables the data subject to access their data;
   6) rectifies and completes personal data;
   7) erases data;
   8) restricts data processing;
   9) notifies the data subject of any rectification or erasure of personal data or restriction of processing;
   10) facilitates data portability.

**§ 4.**

1. The Controller assigns roles and responsibilities in the data processing procedure to each participant involved in the process.

2. Before granting access to personal data, the Controller ensures that every Employee, Associate, or other person processing data under its authorisation is familiarised with the procedures and rules concerning personal data protection that apply at the Controller.
3. The processing of personal data by Employees and Associates may take place only on the basis of documented authorisation from the Controller, the scope of which corresponds to the assigned role and level of responsibility. Furthermore, the Controller requires authorised persons to maintain the confidentiality of data and information on data security measures, as well as to comply with data protection procedures and policies applicable within the Controller's organisation.
4. The Controller identifies personal data resources, data classes, relationships between data resources, and identifies the purposes and methods of data use, in particular by: cases of processing sensitive data, cases of processing unidentified data, and profiling.
5. The Controller verifies whether any situations of joint controllership of personal data occur.
6. Personal data processed by the Controller is collected in personal data sets.
7. The Controller does not undertake processing activities that may involve a high likelihood of a high risk to the rights and freedoms of individuals. If the Controller plans such activities, it will carry out the actions specified in Article 35 et seq. of the GDPR.
8. When planning new processing activities, the Controller analyses their impact on the protection of personal data and incorporates data protection considerations at the design stage.

**§ 5**

1. The Controller maintains a Record of Processing Activities (RoPA), hereinafter the "Record", which constitutes Annex No. 4 to this Policy.
2. In the Record, for each processing activity that the Controller considers separate for the purposes of the Record, the Controller shall record at least:
    a) the name and surname or business name and contact details of the Controller and any joint controllers, and where applicable – the Controller's representative and the Data Protection Officer,
    b) the name of the processing activity,
    c) the purpose of the processing,
    d) a description of the categories of data subjects,
    e) a description of the categories of data,
    f) the legal basis for processing, including specifying the category of the Controller's legitimate interest when legitimate interest is the basis,
    g) the method of data collection,
    h) a description of the categories of recipients of personal data (including processors),

i) information on transfers outside the EU/EEA,

j) a general description of the technical and organisational security measures.

3. The template of the Record contains optional columns. Optional columns are completed as needed and when possible, bearing in mind that more detailed content of the Record facilitates the management of GDPR compliance.
4. The Record of Processing Activities is kept in written and electronic form and updated on an ongoing basis by the Data Protection Officer.
5. The Record of Processing Activities specifies the scope of personal data that an ADO employee is authorised to process. This scope depends on the position held by the ADO employee.
6. The Data Protection Officer or the ADO provides the employee with access to the Record of Processing Activities only to the extent of the processing activities the employee is authorised to perform.

**§ 6**

1. The ADO maintains a Register of Categories of Data Processing.
2. The template of the register referred to in paragraph 1 constitutes Annex No. 5 to this Policy.
3. The Register referred to in paragraph 1 includes, among other things, the following information:
    1) the name and surname or business name and contact details of the controller and any joint controllers, and, where applicable, the representative of the controller and the Data Protection Officer;
    2) the categories of processing;
    3) a general description of the technical and organisational security measures (where possible);
    4) the names of third countries or international organisations to which data is transferred;
    5) documentation of appropriate safeguards for personal data transferred pursuant to Article 49(1), second subparagraph, GDPR.
4. The Register of Categories of Data Processing is maintained in written and electronic form and updated on an ongoing basis by the Data Protection Officer.

**§ 7**

1. The ADO applies appropriate IT and technical measures ensuring the protection of processed personal data, corresponding to the degree of risk and the categories of data subject to protection.
2. The ADO applies the following technical measures:

a) the processing of personal data takes place in rooms that are properly secured and adapted for processing;
b) the rooms are secured with monitoring and alarm systems;
c) the rooms are equipped with cabinets providing security for documentation and data carriers;
d) current and archived documentation is stored in areas where personal data is processed, in lockable cabinets.

3. The ADO applies the following organisational measures:
   a) prepares and implements the Policy,
   b) prepares and implements the Information Security Policy for IT Systems,
   c) familiarises every person, before they begin working with personal data, with the legal provisions concerning personal data protection,
   d) regularly trains persons processing personal data in the safe use of devices and software related to the processing and protection of personal data,
   e) requires persons processing personal data to comply with personal data protection rules,
   f) controls the opening and closing of rooms; the first person starting work opens the rooms, the last person closes them and activates the alarm,
   g) ensures that during working hours rooms are not left unattended and, in particular, that no unauthorised persons are present in areas where personal data is processed,
   h) obtains a written declaration from each person authorised to process personal data, confirming that they have been familiarised with the provisions on data protection contained in this Policy, the Information Security Policy for IT Systems, and that they undertake to comply with them,
   i) supervises compliance with all internal regulations and instructions related to the security of people and information resources, as well as the individual responsibilities of persons employed in the processing of personal data, including documents contained in this Policy.

**§ 8.**

1. All persons are required to process personal data in accordance with the applicable legal provisions and with the rules established by the Data Controller in this Policy, the Information Security Policy for IT Systems, as well as other internal documents and procedures related to personal data processing in the Company.
2. All personal data at Centro-chem sp. z o.o. sp.k. is processed in compliance with the data processing principles provided by law:
   1) in every case, at least one legally defined basis for data processing is present;

2) data is processed fairly and transparently;
3) personal data is collected for specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes;
4) personal data is processed only to the extent necessary to achieve the purpose of processing;
5) personal data is accurate and, where necessary, kept up to date;
6) the storage period of the data is limited to the period during which the data remains useful for the purposes for which it was collected; thereafter, the data is anonymised or erased;
7) the information obligation towards the data subject is fulfilled in accordance with Articles 13 and 14 of the GDPR;
8) data is secured against breaches of data protection rules.

**§ 9.**

1. If a personal data breach is identified, the Controller assesses whether the breach may have resulted in a risk to the rights or freedoms of natural persons.
2. A breach or attempted breach of the principles of personal data processing and protection is considered to include, in particular:
    1) a breach of the security of IT systems in which personal data is processed, if such data is processed in IT systems;
    2) the disclosure or facilitation of disclosure of data to unauthorised persons or entities;
    3) failure, even if unintentional, to fulfil the obligation to ensure the protection of personal data;
    4) failure to maintain the confidentiality of personal data and the methods of securing them;
    5) processing personal data in a manner inconsistent with the intended scope and purpose of its collection;
    6) causing damage, loss, uncontrolled alteration, or unauthorised copying of personal data;
    7) infringement of the rights of data subjects whose data is processed.
3. If circumstances indicating a breach of personal data protection are identified, the User is obliged to take all necessary steps to limit the effects of the breach and to immediately notify the Data Controller.
4. In any situation where the breach may have resulted in a risk to the rights or freedoms of natural persons, the Controller reports the breach to the supervisory authority without undue delay—if feasible, no later than 72 hours after becoming aware of the breach. The template for such notification is set out in Annex No. 6 to this Policy.

5. If the risk to the rights and freedoms of natural persons is high, the Controller also notifies the affected data subject of the incident.
6. The Controller ensures that personal data breaches are reported to the Supervisory Authority unless it is unlikely that the breach will result in a risk to the rights or freedoms of natural persons. For this purpose, the Controller requires all persons processing personal data to immediately report any observed personal data breach.
7. In every case, the Controller examines the breach that has occurred and implements appropriate organisational and technical corrective measures.
8. The ADO keeps a register of breach notifications.
9. A breach notification contains the following information:
    1) the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records affected;
    2) the name and contact details of the Data Protection Officer or another designated contact point from whom further information can be obtained;
    3) the possible consequences of the personal data breach;
    4) the measures taken or proposed by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.
10. The ADO documents all personal data breaches, including the circumstances of the breach, its effects, and the corrective actions taken.
11. The ADO may grant a power of attorney to another person, including an employee of the ADO's workplace, to carry out the procedure related to a personal data breach, provided that no conflict of interest exists with the party in which the breach occurred.

**§ 10**

1. The responsibilities of the Data Controller in connection with hiring, terminating, or changing the employment conditions of employees or associates (persons performing tasks for the Controller under other civil-law contracts) include ensuring that:
    a) employees are adequately prepared to perform their duties;
    b) each employee undertakes to keep personal data processed in the company confidential. The "Statement and Commitment of the Person Processing Personal Data to Maintain Confidentiality" constitutes part of the "Authorisation to Process Personal Data."
2. The Controller identifies and verifies the legal bases for personal data processing, in particular by:
    a) maintaining a system for managing consents for personal data processing;

b) inventorying and preparing justifications for cases where personal data is processed based on the legitimate interests of the Controller.

**§ 11**

1. The Controller fulfils its information obligations towards data subjects. In particular, the Controller:
    1) provides data subjects with all information required by law at the time of collecting their personal data, as well as in other situations where the law requires additional information to be provided to data subjects;
    2) ensures documentation of the fulfilment of the obligations referred to in paragraph 1 point 1.
2. The Controller ensures that data subjects may exercise the rights granted to them under the GDPR. In particular, the Controller makes every effort to ensure that the requests of data subjects are fulfilled within the deadlines set by the GDPR and are properly documented.
3. The Controller applies procedures for dealing with personal data breaches, enabling the identification and verification of a breach and, where necessary, its immediate notification to the Personal Data Protection Office and informing the affected data subject.
4. The Controller uses a data minimisation management methodology (privacy by default), which defines principles for: managing data adequacy, regulating and managing access to data, managing data storage periods, and verifying continued data relevance.

**§ 12**

1. The Controller determines the organisational and technical security measures that can be applied and assesses the cost of their implementation.
2. The Controller determines the usefulness of, and applies, measures and approaches such as:
    1) anonymisation;
    2) encryption of personal data;
    3) other cybersecurity measures ensuring the ability to continuously maintain the confidentiality, integrity, availability, and resilience of processing systems and services;
    4) measures ensuring business continuity and disaster recovery, i.e., the ability to quickly restore access to personal data in the event of a physical or technical incident.
3. The Controller ensures an appropriate level of data security, including by:
    1) carrying out risk analyses for processing activities or categories of processing;
    2) conducting Data Protection Impact Assessments where the risk to the rights and freedoms of individuals is high;

3) adapting security measures to the identified risk;
4) implementing an information security management system;
5) managing incidents involving personal data breaches.

**§ 13**

1. Each user is obliged to maintain an appropriate level of security within the scope of their duties and authorisations.
2. Each user is obliged to comply with the "clean desk policy," which means that:
    a) after completing work, all data carriers containing personal data and all paper documents must be stored in a locked cabinet,
    b) each employee may keep on their desk only those documents that are necessary at that particular moment to perform current tasks,
    c) beverages in containers that may spill must not be placed on the desk,
    d) during work, if an unauthorised person enters the room where personal data is processed, documents must be arranged so that personal data cannot be disclosed,
    e) the employee is obliged to destroy unnecessary documents in such a way that the information contained in them cannot be reconstructed, e.g., using a shredder,
    f) after work, only a telephone and office supplies such as a stapler, hole punch, and pen may remain on the desk.
3. Each user is obliged to comply with the "clean screen policy," which means that if an unauthorised person is present in the room where personal data is processed, the monitor must be turned in a way that prevents reading the data or protected with a screen saver.
4. Each user must conduct conversations, including telephone conversations, in such a way that personal data is not disclosed to unauthorised persons.
5. Each user submits a declaration in accordance with the template specified in Annex No. 7 to this Policy, in which:
    a) they confirm that they have read the Act, the Regulation, this Policy, and the Information Security Policy for IT Systems,
    b) they undertake to ensure the protection of the personal data they process.
6. Persons processing personal data using portable computers are additionally obliged to observe the following rules:
    a) during transport, storage, and use of a portable computer, particular caution must be exercised,
    b) personal data located on portable computer drives must be protected cryptographically,
    c) leaving a portable computer unattended in a car, storage room, luggage area, etc. is prohibited,

d) a person using a portable computer must use it in such a manner as to prevent unauthorised persons from viewing the data displayed on the screen,
e) providing a portable computer to unauthorised persons is prohibited.

7. Each user, including after the termination of cooperation with the ADO, is obliged to protect all information concerning processed personal data, the functioning of systems or devices used for personal data processing, and data protection methods.
8. Processing personal data in a manner inconsistent with this Policy is prohibited.
9. Users who do not comply with the principles arising from this Policy, the Information Security Policy for IT Systems, the Act, and the Regulation may, in justified cases, be held liable under applicable law.
10. Unjustified failure by an employee to comply with the acts referred to in paragraph 9 may be treated as a serious breach of the employee's basic duties.
11. Employees are particularly obliged to:
    a) strictly follow the scope of the authorisation granted to them,
    b) process and protect personal data in accordance with legal provisions,
    c) maintain the confidentiality of personal data and the methods used for securing them,
    d) report incidents related to breaches of data security or improper functioning of the system.
12. Employees and Associates who process personal data are particularly obliged to:
    1) process data in accordance with their authorisation[3] and with due diligence;
    2) immediately inform the DPO directly if they observe an event that may constitute a personal data breach;
    3) participate in organised personal data protection training sessions;
    4) maintain the confidentiality of personal data and information on the methods of their protection, in accordance with the signed confidentiality clause.

**§ 14**

1. To ensure the protection of personal data, the Controller may appoint a Data Protection Officer (DPO), in accordance with the guidelines set out in § 1(12) of this Policy. The appointment of the DPO constitutes Annex **No. 9** to this Policy.
2. In carrying out this Policy, the Data Protection Officer (DPO) exercises the highest diligence to protect the interests of data subjects and, in particular, ensures that personal data is:

[3] Annex No. 8

1) processed lawfully;
2) collected for specified, lawful purposes and not further processed in a way incompatible with those purposes;
3) factually correct and adequate in relation to the purposes for which it is processed;
4) stored no longer than necessary to achieve the purposes for which it was collected.

3. The responsibilities of the Data Protection Officer (DPO) include:
    1) informing the controller, the processor, and employees who process personal data about their obligations under the GDPR and other Union or Member State data protection provisions, and providing them with advice on these matters;
    2) monitoring compliance with the GDPR, other Union or Member State data protection provisions, and the controller's or processor's personal data protection policies, including the assignment of responsibilities, raising awareness, training personnel involved in processing operations, and conducting related audits;
    3) providing recommendations, upon request, on Data Protection Impact Assessments and monitoring their implementation in accordance with Article 35 GDPR;
    4) cooperating with the supervisory authority;
    5) acting as a contact point for the supervisory authority on issues related to processing, including prior consultations under Article 36 GDPR, and conducting consultations on any other relevant matters when appropriate;
    6) acting as a contact point for data subjects in all matters related to the processing of their personal data and the exercise of their rights under the GDPR;
    7) maintaining the record of processing activities or the record of categories of processing activities.
4. The DPO has the right to:
    1) designate, recommend, and enforce the performance of tasks related to personal data protection across the entire organisation;
    2) access premises where personal data sets are located and conduct necessary examinations or other control activities to assess compliance of data processing with the GDPR, and to request written or oral explanations to the extent necessary to determine the factual state;
    3) request the presentation of documents and all data directly related to the subject of the inspection;
    4) request access to devices, data carriers, and IT systems used for personal data processing.
5. The DPO performs their tasks with due regard to the risks associated with processing operations, taking into account the nature, scope, context, and purposes of the processing.

6. Data subjects may contact the DPO in all matters related to the processing of their personal data and the exercise of their rights under the GDPR via the following email address:

**iod@centro-chem.pl**

**§ 15**

1. The disclosure of personal data is permitted only where one of the conditions referred to in Article 6(1) or Article 9(2) of the GDPR is fulfilled. In case of doubt as to whether personal data should be disclosed, the DPO must be consulted.
2. Entrusting the processing of personal data to a third party is carried out on the basis of a data processing agreement, after verification of that entity in the manner specified in the Policy for Selecting a Data Processing Supplier.
3. The template of the agreement referred to in paragraph 3 constitutes Annex No. 10 to this Policy.
4. The list of entities to which personal data processing has been entrusted is included in Annex No. 11 to this Policy.
5. Personal data processed by the ADO may be disclosed to the data subject or to other entities authorised by the data subject.
6. Furthermore, personal data may be disclosed to other entities only for the purpose of performing a contract concluded between the ADO and the data subject, or to entities authorised by law.

**§ 16**

1. The Controller continuously verifies whether personal data is being transferred to third countries (i.e., outside the European Economic Area) or to international organisations.
2. In the event of transferring personal data to third countries or international organisations, the Controller ensures that such transfers comply with the GDPR.
3. The Controller continuously verifies whether cross-border personal data processing occurs.

**§ 17**

1. The area in which personal data is processed at Centro-chem sp. z o.o. sp.k. includes files, indices, logs, registers, and other record collections located in the office premises situated in Turka, Turka 141B, 20-258 Lublin.The list of rooms or parts of rooms that constitute the area in which personal data is processed is provided in **Annex No. 12** to this Policy.
2. Additionally, the area in which Personal Data is processed includes all portable computers and other data carriers located outside the area indicated above.

3. The Administrator ensures the application of technical and organisational measures necessary to ensure the confidentiality, integrity, accountability, and continuity of the processed data.
4. The applied security measures (technical and organisational) must be adequate to the identified level of risk for specific systems, types of data sets, and categories of data. The measures include:
    1) restricting access to rooms where personal data is processed exclusively to duly authorised persons. Other persons may remain in these rooms only when accompanied by an authorised person;
    2) locking the rooms forming the personal data processing area during employees' absence in a manner that prevents access by third parties;
    3) using lockable cabinets and safes to secure documents;
    4) using shredders for effective destruction of documents containing personal data;
    5) protecting the local network from external actions using a firewall;
    6) creating backup copies of data on portable drives secured with passwords;
    7) protecting computer equipment used by the administrator against malicious software;
    8) securing access to devices located at the company's premises with passwords;
    9) using data encryption during transmission.

5. The Administrator implements appropriate measures to ensure that communication with the Data Subject is provided in a concise, transparent, and easily accessible form.
6. Receiving and handling Data Subjects' requests is carried out in accordance with the provisions of this Policy for handling Data Subject requests related to the exercise of rights associated with data processing.

**§ 18**

1. The Administrator ensures continuous monitoring of the Company's compliance with personal data protection rules.
2. The DPO is responsible for taking actions related to ensuring compliance. Every employee and associate of the Company is obliged to support the DPO in performing their tasks, in particular by providing necessary information and explanations.

**§ 19**

**Information Security and Personal Data Protection in Remote Work**

1. The following procedure describes how to ensure information security and personal data protection in the context of remote work.
2. It is assumed that the Employee undertakes to secure access to work equipment and any data and information they possess (including those on paper) against third parties, including individuals living in the same household.
3. Performing work remotely does not release the employee from the obligation to comply with the provisions of the Company's Personal Data Protection Policy and related documents, including the Information Security Policy for IT Systems. The employee is required to submit a declaration confirming compliance with these regulations.
4. The employee uses the access data provided by the employer (including logins and passwords) to IT systems and email, and ensures the protection of this data as well as the personal data and information processed through such access, particularly against access by unauthorised persons, destruction, or loss.
5. The employee must report all security incidents and personal data protection breaches, as well as any suspicion of such incidents or any irregularities in data protection, to the persons responsible for personal data protection and information security in the workplace.

**§ 20**

1. Devices and software provided by Centro-chem sp. z o.o. sp.k. for remote work are to be used exclusively for performing professional duties.
2. The employee is required, in particular, to:
    1) avoid installing additional applications or software that are not compliant with the security procedure;
    2) ensure that all devices used have the necessary updates to the operating system (iOS or Android), software, and antivirus system;
    3) designate an appropriate workspace so that third parties cannot access documents the employee is working on. Whenever leaving the workstation, the employee must lock the device they are working on;
    4) secure the computer by using strong passwords and multi-factor authentication, which will limit access to the device, and at the same time reduce the risk of data loss in the event of theft or loss of the device.

**§ 21**

1. As part of remote work, the Administrator may carry out inspections regarding information security and data protection procedures, including personal data protection.

2. The inspection includes, in particular:
    1) checking how the employee complies with the applicable personal data protection rules adopted by the employer, including the use of required security measures;
    2) confirming the employee's participation in personal data protection training;
    3) confirming the application of the personal data protection procedures in force at the employer;
    4) checking the tools and systems through which the employee accesses the employer's personal data.

3. Conducting an inspection to verify compliance with the security and information protection requirements, including personal data protection procedures, consists in checking, in particular:
    1) whether the employee communicates with the employer and other employees using official email accounts;
    2) whether personal data has not been disclosed to unauthorised persons;
    3) whether the employee uses IT systems provided by the employer in which personal data is processed;
    4) whether the room in which personal data is processed ensures protection against unauthorised access by third parties, in particular whether the positioning of the monitor ensures the confidentiality of personal data;
    5) whether the employee knows the procedures and deadlines for reporting data protection incidents and suspected incidents;
    6) whether the employee knows the identity and contact details of persons responsible for information security and personal data protection;
    7) whether the employee applies organisational and technical measures necessary for personal data protection, adopted within the organisation, such as encryption or pseudonymisation;
    8) whether unsecured documentation containing personal data is present in the employee's surroundings;
    9) whether the employee regularly deletes unnecessary personal data and destroys unnecessary working documentation.
4. Monitoring proper compliance with security and information-protection rules, including personal data protection procedures, is carried out using electronic communication tools and may also take place at the location where remote work is performed.
5. The inspection referred to in paragraph 3 may be carried out using electronic communication tools, including through or with the use of:

1) the business telephone provided to the employee;
2) the business email account;
3) communication tools or internal chat systems used in the workplace

— during the employee's working hours, without prior notice from the employer.

6. As part of an inspection conducted using electronic communication tools, the employer may request an online meeting with the employee, which includes mutual disclosure of images and of the environment in which the employee performs remote work. The employee must ensure that no family members or other individuals present in the household appear in the background.
7. Detailed rules for organising and controlling personal data protection in remote work are defined in the *Personal Data Protection Procedure for Remote Work* at Centro-Chem Sp. z o.o. Sp.k.

**§ 22.**

**Use of Cookies**

1. The following procedure describes how cookies are used by the User when using the Service, understood as the website operated by the Administrator at:

   https://www.centro-chem.pl.

   The User is any natural person visiting the Service or using one or more of its services or functionalities.
2. In connection with the User's use of the Service, the Administrator collects data necessary to provide individual services offered.The Administrator uses the following categories of cookies:
   a) **Necessary (technical) cookies** – used for the correct functioning of the website, do not require the User's consent, enable e.g. logging in, maintaining sessions, filling in forms,
   b) **Analytical and statistical cookies** – used to analyse the functioning of the Service, may originate from the Administrator or external providers, require the User's consent before being activated,
   c) **Marketing and advertising cookies** – used for profiling, remarketing, and personalising advertising content, and may be transferred to external providers (e.g. Google, Meta); they require the User's explicit consent in accordance with EDPB and UODO guidelines,
   d) **Functional cookies** – enable remembering User settings (e.g., language, preferences); they are activated only upon consent, unless they are technically necessary.

3. Personal data provided by the User in the Service or collected by the Administrator about the User is processed in accordance with the GDPR, the Personal Data Protection Act, and other legal acts regulating personal data protection at the national and European levels.
4. The Administrator uses technical measures required by applicable data protection regulations to prevent unauthorised persons from acquiring or modifying personal data transmitted electronically via the Service.
5. Personal data of all individuals using the Service is processed by the Administrator for the following purposes:
    1) **providing electronic services**, including making available to Users the content stored on the Service — the legal basis for processing is the necessity to perform a contract (Art. 6(1)(b) GDPR);
    2) **establishing, pursuing, or defending against claims** — the legal basis is the Administrator's legitimate interest (Art. 6(1)(f) GDPR), consisting in protecting its rights.
6. The Administrator provides the ability to contact them using an electronic contact form. Using the form requires providing Personal Data necessary to establish contact with the User and respond to the inquiry.
7. Personal data is processed to identify the sender and handle their inquiry submitted via the contact form — the legal basis for processing is the necessity to perform a service contract (Art. 6(1)(b) GDPR); for optional data, the legal basis is consent (Art. 6(1)(a) GDPR).
8. The User's personal data may also be used by the Administrator to send them marketing content through various channels, such as email or MMS/SMS. Such actions are taken ONLY if the User has given consent, which may be withdrawn at any time.
9. The Administrator may use tools from external providers, such as: **Google Analytics, Google Ads, Meta Pixel (Facebook), remarketing tools.**
10. In every case:
    1) the provider acts as a data recipient or processor;
    2) data transfer to third countries is carried out in accordance with the GDPR;
    3) Standard Contractual Clauses (SCC) are applied;
    4) Transfer Impact Assessments (TIA) are conducted where required.

11. The Administrator applies the following retention periods:
    a) **session cookies** – until the browser is closed,
    b) **persistent cookies** – up to 12 months,
    c) **cookie consents** – up to 24 months.
12. The User may withdraw their consent through:
    a) the cookie settings panel available on every page of the Service (link in the footer),
    b) changing browser settings,
    c) contacting the Administrator.

Withdrawal of consent does not affect the lawfulness of processing carried out before its withdrawal.

13. The Administrator implements technical and organisational measures ensuring:
    a) blocking external scripts prior to consent,
    b) encryption of data transmission (HTTPS),
    c) minimisation of data transferred to service providers,
    d) limiting data retention to the minimum necessary.
14. Detailed rules for the processing of Users' personal data and the duration of such processing are defined in the Privacy Policy available at:

https://centro-chem.pl/polityka-prywatnosci/

## § 23.

## Transfer of Data Outside the European Economic Area

1. SAFThe Administrator may transfer personal data outside the European Economic Area (EOG/EEA) only when necessary and only with the assurance of an adequate level of protection, primarily through:
    1) cooperation with entities processing personal data in countries for which the European Commission has issued an adequacy decision;
    2) applying the Standard Contractual Clauses (SCC) issued by the European Commission;
    3) applying Binding Corporate Rules approved by the competent supervisory authority;

4) in the case of transfers to the USA – cooperation with entities participating in the Privacy Shield programme approved by the European Commission.

2. The Administrator always informs about the intention to transfer personal data outside the EEA at the stage of data collection.
3. The Administrator is required to conduct a Transfer Impact Assessment (TIA) for every transfer of data outside the EEA.

**§ 24.**

**Privacy Procedure for Job Candidates at Centro-chem Sp. z o.o. Sp.k**

1. The following procedure contains information about the personal data collected by Centro-chem Sp. z o.o. Sp.k – the Administrator – in connection with recruitment processes. It applies to the personal data of candidates for employment at the Company, regardless of the legal basis for the employment relationship.
2. For the purpose of conducting its business, the Company collects and uses information identifying natural persons – personal data – including information about future, current, and former employees as well as individuals cooperating under civil law contracts.
3. This policy applies to all forms of use ("processing") of personal data of candidates for employment at the Company ("Candidates"), regardless of the legal basis for employment. The information clause regarding the processing of personal data of job candidates at Centro-chem Sp. z o.o. Sp.k constitutes **Annex No. 13** to this Policy.
4. For recruitment purposes, Centro-chem Sp. z o.o. Sp.k collects the basic data indicated in Article $22^1$ § 1 Act of 26 June 1974, the Labor Code[4], such as first name(s) and surname, date of birth, education, employment history, as well as other personal data if necessary to fulfil a legal obligation imposed on the employer. Providing this data is a statutory requirement (for Candidates applying for employment under an employment contract). Failure to provide the data results in the inability to establish employment and the inability to conduct the recruitment process.
5. Personal data processed by Centro-chem Sp. z o.o. Sp.k may also include special, particularly sensitive categories of data, such as information regarding disability status. Such categories of data will be subject to special protection by the Company and will not be disclosed to unauthorised persons.

[4] Act of 26 June 1974, the Labor Code (Journal of Laws of 2025, item 277, as amended)

6. Centro-chem Sp. z o.o. Sp.k may also collect Candidates' personal data from entities providing recruitment services or employment agencies, outplacement agencies, university career offices, as well as online platforms (including dedicated social networking sites linking employers with job candidates), provided that there is an appropriate legal basis for doing so. When obtaining such information, the Company will not excessively interfere with the Candidate's privacy and will limit itself only to personal data from the professional sphere and will process such data solely for purposes related to conducting recruitment.
7. Centro-chem Sp. z o.o. Sp.k processes personal data only when:
    1) **the processing is necessary to fulfil contractual obligations** towards Candidates or, at the Candidate's request, is necessary to take specific steps prior to entering into a contract, including conducting the recruitment process;
    2) **the processing is required to comply with legal obligations**, or is directly mandated by law (e.g., Article $22^1$ of the Labour Code);
    3) **the processing is necessary for the legitimate interests** pursued by the Company or a third party and does not excessively interfere with the Candidate's interests or fundamental rights and freedoms. The Company strives to maintain a balance between its legitimate interests and the Candidate's privacy. Such "legitimate interests" include:
        a) fulfilling the Company's corporate and social responsibility goals,
        b) establishing or pursuing civil-law claims within the Company's business operations, as well as defending against such claims,
        c) taking measures necessary to maintain operational continuity (e.g., workforce planning, budgeting, planning workspace, etc.);
    4) in some cases, when the Company has obtained prior consent from the Candidate.
8. Special categories of personal data may be processed by the Company only in specific cases, i.e., when processing is necessary to fulfil obligations arising from employment, social security, or social protection — this applies particularly to data concerning disability status and related entitlements.

**§ 25.**

1. If the Company processes a Candidate's personal data on the basis of consent, such consent may be withdrawn at any time in a manner as easy as it was given. Failure to provide consent for data that Candidates are not legally required to submit will not result in refusal to establish employment, and withdrawal of consent will not have negative consequences for the Candidate.
2. The Company processes the Candidate's personal data **for a specific purpose** and processes only the data necessary to achieve that purpose.
   In particular, the Company processes Candidates' personal data for the following purposes:
   1) conducting recruitment activities;
   2) preparing employment agreements for Candidates;
   3) managing employment documentation;
   4) complying with all legal obligations imposed on the Company with respect to Candidates.
3. The Company may transfer personal data to recipients and other third parties in order to fulfil the purposes listed in paragraph 2, to the extent necessary for them to perform tasks commissioned by the Company or when required by law.
   Recipients or third parties may include:
   1) **Entities processing personal data on behalf of the Company**, such as:
      a) providers of IT systems and hosting services to the Company,
      b) entities providing document archiving services.

These entities do **not** independently decide how Candidate personal data is processed. They process such data only to the extent necessary for the Company's operations. The Company exercises control over their actions through contractual provisions that protect Candidate privacy.

   2) Entities such as:
      a) recruitment agencies or temporary employment agencies,
      b) legal or tax advisors,
      c) courier or postal service providers.

Such entities act as **independent data controllers**. This means that the Company has no influence over how and for what purposes they process Candidate data. The Company is not responsible for whether these entities comply with applicable regulations.

3) any national public administration authorities, authorities of other EU member states (e.g., data protection authorities in other EU countries), or courts, if required by national or EU law or upon their request.

4. Personal data transferred within the Company may also be processed in a country **outside the EEA**, which consists of EU member states, Iceland, Liechtenstein, and Norway. Countries outside the EEA may not provide the same level of data protection as EEA countries.
5. If Candidate personal data is transferred outside the EEA in the future, the Company will implement appropriate safeguards to ensure such transfers comply with applicable data protection regulations. To ensure an adequate level of protection, the Company may, for example use a data processing agreement with the third-party recipient based on Standard Contractual Clauses approved by the European Commission, or ensure that the transfer is made to a jurisdiction covered by a European Commission adequacy decision.
6. The Company stores personal data only for as long as necessary to achieve the purpose for which it was collected, or for as long as required by law.
7. Candidates' personal data is processed for the duration of the recruitment process. After that time, personal data relating to the recruitment process will be processed for the period of limitation of civil-law claims, in order to enable the Company to defend itself against potential claims or to pursue such claims, if there is a risk that such claims may be brought by or against the Company. Under Polish law, this period is, as a rule, no longer than 3 years from the end of the recruitment process.
8. If a Candidate wishes their personal data to be removed from the Company's databases, they may submit a request in accordance with the information described in paragraph 10.
9. The Candidate has the right to access their personal data processed by the Company. If the Candidate believes that any information concerning them is incorrect or incomplete, they also have the right to request its rectification in the manner specified in paragraph 10 below.
10. The Candidate also has the right to:
    1) withdraw consent where the Company has obtained such consent for the processing of personal data (provided that such withdrawal does not affect the lawfulness of processing carried out before the withdrawal);
    2) request the erasure of personal data;

3) request the restriction of the processing of personal data;
4) object – on grounds relating to their particular situation – to the processing of personal data (including profiling), where such processing is carried out for the purposes of performing a task in the public interest or for the purposes of the legitimate interests of the Company or a third party;
5) data portability, i.e. to receive personal data provided to the Company in a structured, commonly used, machine-readable format and to request that such data be transmitted to another data controller, without hindrance from the Company and subject to the Company's own confidentiality obligations.

11. The Company will assess Candidates' requests, demands, or objections in accordance with applicable data protection laws. These rights are not absolute; the law provides for exceptions to their application.
12. Candidates may exercise the above rights by contacting the Company by post at: **Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa, Turka 141B, 20-258 Lublin**, or by sending an email to: **iod@centro-chem.pl**.

## § 26.

## Data Protection Impact Assessment (Risk Analysis)

1. A Data Protection Impact Assessment (DPIA) is a formal procedure defined in Article 35 of the GDPR, which involves conducting a risk analysis for which the Data Controller (ADO) is responsible. If the ADO is not required to perform a DPIA, they may still use the procedure below to conduct a risk analysis in order to demonstrate accountability and compliance with GDPR requirements. If a Data Protection Officer (DPO) has been appointed, the DPIA must be carried out **with their involvement**.
2. The risk analysis is conducted in the last quarter of each year according to the methodology attached to this document (PIA methodology).
3. As part of the DPIA (risk analysis), the Administrator must fulfil their legal obligations concerning the data within the datasets. In particular, the Administrator must ensure that:
    1) the data is processed lawfully (on the basis of Articles 6 and 9 GDPR);
    2) the data is adequate in relation to the purposes of processing;
    3) the data is processed for a specific period (data retention);

4) data subjects have been provided with the required information (Articles 12, 13, and 14 GDPR), including their rights (e.g., right of access, data portability, rectification, erasure, restriction of processing, objection, withdrawal of consent);
5) information clauses for these persons have been prepared;
6) data processing agreements with processors exist (Article 28 GDPR).

**§ 27.**

**Risk Analysis**

1. This procedure describes how to conduct a risk analysis to ensure the protection of personal data appropriate to identified threats arising from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access to personal data.It is assumed that the risk analysis is carried out for a dataset or group of datasets (categories of persons) or for processing activities (e.g., employee dataset, customer dataset, process of sending commercial information from a marketing database).
2. Whenever this procedure refers to the terms mentioned in paragraph 1 without further specification, it means:
    1) **Assets** – this refers to material and non-material resources that affect the processing of personal data;
    2) **Personal data breach (Incident)** – this refers to a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data transmitted, stored, or otherwise processed;
    3) **Threat** – this refers to a potential breach (a potential incident);
    4) **Impact** – this refers to the consequences of an undesirable incident (losses in the event a threat materialises);
    5) **Risk** – this refers to the likelihood that a specific threat will occur and cause losses or damage to assets.
3. When identifying threats:
    1) The Administrator is responsible for determining a list of threats to confidentiality, availability, and integrity that may occur during the processing of data within a dataset, for a category of persons, or within a processing activity;
    2) Threats must be identified in relation to previously identified assets.

4. Risk assessment for identified threats includes:
    1) The Administrator determines the **Probability (P)** of occurrence of each threat within the dataset (or category of persons) or processing activity. The established probability scale is shown in **Table A**;
    2) The Administrator determines the **Impact (S)** of incidents (materialisation of threats), taking into account financial losses, reputational damage, sanctions/penalties. The established impact scale is shown in **Table B**;
    3) The Administrator calculates the **Risk (R)** for all threats and their impacts using the formula:

$$\mathbf{R = P \times S}$$

| **Table A**<br><br>**Probability of occurrence of a threat (P)** | **Scale (Weight)** |
|---|---|
| low probability | 1 |
| medium probability | 2 |
| high probability | 3 |

| **Table B**<br><br>**Impact of occurrence of a threat (S)** | **Scale (Weight)** |
|---|---|
| small impact (up to 10,000 PLN, local press incident) | 1 |
| medium impact (10,000 – 100,000 PLN, national press incident) | 2 |
| **large impact** (from 100,000 PLN, violation of law) | 3 |

5. Comparing the calculated risks with the scale and determining further risk-handling actions includes:
    1) The Administrator compares the calculated risks with the established scale and makes decisions regarding further risk management;
    2) The established Risk Scale is presented in Table C.

| **Table C – Risk Level** | Value<br><br>**(R = P ×S)** |
|---|---|
| negligible and acceptable risk (accepted) | **1 – 2** |
| optional risk (may be accepted or reduced) | **3 – 6** |

| | |
|---|---|
| unacceptable risk (must be reduced) | 9 |

6. Response to the assessed risk value includes:
    1) **Risk acceptance** – safeguards are adequate, and no additional measures are required;
    2) **Risk-reducing actions** that the Administrator may apply:
        a) **Transfer** – shifting the risk (outsourcing, insurance),
        b) **Avoidance** – eliminating activities that create risk (e.g., prohibition on taking laptops outside the organisation),
        c) **Reduction** – applying safeguards to reduce risk (e.g., encrypting USB drives containing data taken outside the company)
    3) The risk analysis is carried out using a designated template (internal organisational documents).
7. Re-assessment of risk is conducted periodically or after significant changes in data processing (e.g., processing new datasets/categories of persons, implementation of new processing operations, legal changes).
8. Risk management also includes a Risk Treatment Plan, which consists of:
    1) wherever the Administrator decides to reduce risk, a list of safeguards to be implemented is defined, along with deadlines and responsible persons – forming the Risk Treatment Plan (internal organisational documents);
    2) The Administrator is required to monitor the implementation of the safeguards.

## § 28.

## Period of Personal Data Processing

1. The period of data processing by the Administrator depends on the type of service provided and the purpose of processing. The processing period may also result from legal provisions when they constitute the basis for processing. In the case of processing based on the Administrator's legitimate interest, the data is processed for the period necessary to fulfil that interest or until an effective objection to processing is lodged. If processing is based on consent, the data is processed until such consent is withdrawn.

When the basis for processing is the necessity to conclude and perform a contract, the data is processed until the contract is terminated.

2. The processing period may be extended if the data is necessary for establishing, pursuing, or defending against claims. After that period, data may be retained only if and to the extent required by law. Once the processing period has expired, the data is irreversibly deleted or anonymised.

## Chapter III

## Final Provisions

### § 29

1. An employee who fails to fulfil the obligations arising from this document shall bear responsibility under the Labour Code, data protection regulations, and the Criminal Code with respect to personal data covered by professional secrecy.
2. Procedures for granting authorisations, authentication methods and measures, and backup creation procedures are regulated by the Instruction for Managing the IT System Used for Personal Data Processing.
3. Updates to this Policy are made by the Administrator, who submits all proposed changes to the entity responsible for its implementation.
4. This Policy enters into force on the date of signing the Management Board Resolution.
5. This Policy may be subject to further amendments. If required by law, any information regarding future changes or additions to the processing of personal data described in this Policy will be communicated via the communication channels commonly used within the Company.
6. The Annexes constitute an integral part of this Security Policy.