DATA PROTECTION POLICY
OY CHEMEC AB

1 INTRODUCTION

This document describes the data protection policy and its implementation and monitoring processes of Oy Chemec Ab.

Oy Chemec Ab commits to comply with the existing Finnish data protection and personal data legislation, including EU General Data Protection Regulation (GDPR), as well as other applicable acts and laws regarding personal data processing. Oy Chemec Ab is also committed to process personal data based on the best practises on data management and data processing.

A data protection policy aims at safeguarding the legal rights of the organisation's customers, employees, and other stakeholders with regard to the processing of their personal data and ensuring the processor's rights and obligations when processing personal data.

When processing personal data, data protection includes individuals' privacy protection and their other rights that safeguard privacy protection. When implementing data protection, special attention is paid on the privacy and confidentiality of personal data, prevention of unauthorised access to the data and prevention of the use of the data in a way that harms the affected person.

This data protection policy is the main document guiding data protection in the organisation and it is accessible to all employees.

CONTROLLER

Oy Chemec Ab, business ID FI19084427, Ahventie 4 A 21-22, 02170 Espoo, Finland

CONTACT PERSON IN DATA PROTECTION RELATED MATTERS

The contact person for all data protection related matters is Petri Ratala. He can be contacted by e-mail: petri.ratala@chemec.fi or phone: +358 40 536 8877.

2 DEFINITIONS

Personal data – All information that can be used to identify a person directly or indirectly, such as by combining an individual data item with some other piece of data that enables identification, and any information relating to an identified or identifiable natural person.

Data subject – An identified or identifiable natural person whose personal data is stored by the organisation.

Register / Data file / Filing system – Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralized or dispersed on a functional or geographical basis. A data file is composed of all personal data processed for the same purpose of use regardless the form of processing (manual, electric or combination) and the information system(s) and/or archives used for the processing and storage.

Controller –The natural or legal person, public authority, agency, or other body who determines the purposes and means of the processing of personal data.

Processor – The third party that processes personal data on behalf of a controller.

Processing – Any operation or set of operations which is performed on personal data or on sets of personal data using either automatic or manual data processing, such as collection, storage, alteration, retrieval, use, dissemination, erasure, or destruction.

GDPR (General Data Protection Regulation) – Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN; a law regulating the processing of personal data, which was adopted in all EU countries in the spring of 2018.

Personal data breach – An event leading to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data. Examples of personal data breaches include lost data transfer device (such as USB memory stick), stolen computer, hacking, malware infection, cyber attack, fire in the data centre, or disclosing a document containing personal data to a wrong person.

3 PROCESSING OF PERSONAL DATA AND ITS SECURITY

The data protection principles which are followed when processing personal data in the organisation are described in the table below.

Principle	Description
Lawfulness, fairness and transparency	Collect personal data only when it is justifiable. Do not collect personal data secretly or in an unexpected manner.
Purpose limitation	Do not process personal data for any other purpose than the one it has originally been collected for.
Minimisation of data	Do not process unnecessary or excessive personal data. Personal data must always be necessary.
Accuracy of data	Outdated, inaccurate or incorrect data must be rectified or erased without delay.
Storage limitation	Do not store personal data any longer than necessary. Erase all data that has become unnecessary.
Integrity and confidentiality	Ensure the security of personal data both in physical and electronic environment.

The access to the data files is restricted to ensure that the data usage is only available and entitled to only those employees, who on behalf of their work are entitled to use the systems containing that data and need to process the data for their duties.

The data content within the filing systems is restricted to minimum in accordance with the mandatory needs and the purpose of use. The personnel are directed to process personal data appropriately. The accuracy of data is ensured whenever possible and data is updated whenever necessary.

Data systems used for processing personal data have adequate technical protection. The access to those data systems is restricted with appropriate measures including personal usernames and passwords. The data is backed up securely. Any material containing personal data is destroyed securely.

Processing and storing of personal data is partially outsourced to external service providers with written contracts. The controller ensures that such outsourcing is in accordance with applicable data protection legislation and personal legislation, and that those external service providers do not use the personal data for their own purposes.

Personal data is not transferred outside the controller or its external service providers storing the data in a manner enabling the data to be identified, except in the following exceptional circumstances: if required by any law or ruling of a governmental or regulatory authority or court, or if it is otherwise necessary for the purposes of preventing or investigating any breach of law, user terms or good practices or to protect the rights of the controller or a third party.

All data files that are controlled by Oy Chemec Ab are listed in the Data Inventory document which includes the following information per each data file:

- Name of the data file
- Categories of data subjects
- Personal data
- Data sources
- Location of the data
- Purpose of the processing
- Legal basis for the processing
- Sensitive data
- Owner
- Amount of data
- Processors
- Transfers to any third parties or outside EU, access to data
- Storage period and destruction responsibilities
- Protection and category of data

There is a privacy notice document available for each of the data files listed in the data inventory.

4 RISK ASSESMENT AND MANAGEMENT

The data files controlled by Oy Chemec Ab do not typically include sensitive or other high risk data except the trade union membership information and limited health information of its personnel. Oy Chemec Ab pays special attention to the confidentiality of personal data, to disabling unauthorised access to the data, and to the appropriate processing of the data with no harm to the data subject.

Assessment of data protection related risks is included in the general ISO9001 risk management process used in the organisation. Within that process the risks and the actions for managing them are identified and assessed. More information can be found in the internal document called Personal data risk assessment and management (Only in Finnish: Tietosuojariskien arviointi ja hallinta).

5 DATA PROTECTION AWARENESS

The management of Oy Chemec Ab is responsible for ensuring that employees have essential knowledge about personal data processing needed for their job description and adequate resources for going through data protection related training if necessary. The management is also responsible for providing potential supplemental or advanced training for those persons who are identified to particularly need it.

In the beginning of their employment new employees receive introduction to personal data processing and complying with applicable acts and laws regarding personal data processing. This ensures that all personnel have necessary knowledge about protection needed and processes to be followed e.g. related to computer protection and passwords.

There is an internal document available to personnel called Data protection instructions where the directions and procedures related to personal data processing are documented.

6 RIGHTS OF THE DATA SUBJECTS

According to the General Data Protection Regulation (GDPR), data subjects have certain rights regarding their personal data. As a controller, Oy Chemec Ab ensures that these data protection rights are fulfilled. The data subjects can exercise their rights by sending a signed letter or similarly confirmed document to the contact person in data protection related matters, who can then request the data subject to visit the controller's premises to provide personal identification and possible mandate or other documentation confirming the rightful access to the request. The access request can be made free of charge once a year.

The data subject has a right of access to their personal data as well as to demand the rectification of inaccurate personal data concerning them and to have incomplete personal data completed.

If the data subject has given their explicit consent for personal data processing, they have anytime the right to withdraw that previously given consent. This consent includes the cases where the data subject has spontaneously sent their data to the controller for example for recruitment purposes.

The data subject also has a right to ask the controller erase data concerning them if the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or the controller has no legal basis for processing or storing the data. Furthermore, the data subject has a right to request the controller to restrict or object to the processing of their personal data. They also always have the right to lodge a complaint with a supervisory authority concerning the circumstances related to the processing of their personal data.

All the requests related to these rights are documented in the internal Register of Measures on Data subjects' rights document, handled appropriately, and responded in a timely manner, no later than within one month of the receipt of the request. The document is maintained by the organisation's contact person in data protection related matters.

Register of Measures on Data subjects' rights

The internal Register of Measures on Data subjects' rights document is recorded in order to be able in practise to demonstrate Oy Chemec Ab's compliance with the data protection legislation concerning the rights of the data subjects.

The document is stored and updated in myGDPR service, and it includes at least the following information about each request:

- Date of the request
- Recipient of the request
- Name and contact information of the data subject
- Type and description of the request
  - Data request / Deletion of data / Prevention of profiling / Transfer of the data
- Proof of identity
  - If the requesting person acts on behalf of someone else, proof of the mandate

- Performed actions
- Date of the response

7 PROCEDURES FOLLOWED BY A DATA BREACH

If data privacy is suspected or confirmed to be compromised the situation will be investigated and the necessary measures will be taken without delay. All personal data breaches, their effects and the remedial actions taken are documented. If there are several reports about data breaches, they will be taken care of in the order of their importance.

Any suspected or confirmed data breach must be immediately reported by contacting the organisation's contact person in data protection related matters who will record it into the internal Register of data breaches document at myGDPR service and assess the level of risk caused to the individuals concerned as well as possibly necessary remedial actions. Actions will be taken based on the risk assessment, following one or more of the following three steps:

1. No risk:

If the data breach is not likely to cause any risk to the rights and freedoms of natural persons, the breach, its effects, and the remedial actions taken shall be documented for organisation's internal use.

Register of data breaches

The Register of data breaches document is recorded to be able to in practise demonstrate Oy Chemec Ab's compliance with the data protection legislation concerning the data breaches. The register is part of the documents, procedures and responsibilities process as well as the systematic descriptions related to managing the data breaches.

The document stored and updated in myGDPR service and it includes at least the following information about each breach:

- Date of detecting the breach
- Description of the nature of the data breach
- Logical units of personal data affected by the data breach
- Estimated number of data subjects affected by the data breach
- The likely consequences of the data breach
- All measures taken or intended to be taken to address the data breach, including measures to mitigate the breach

2. Risk:

If a personal data breach can cause a risk to the rights and freedoms of natural persons, the supervisory authority must be notified, in addition to the internal documentation. This notification must be done without undue delay and, where feasible, not later than 72 hours after the controller has become aware of the data breach.

Notification to the supervisory authority

Oy Chemec Ab will assess the risks caused by the data breach to the rights and freedoms of data subjects immediately after detecting the breach. If those risks are likely, the supervisory authority will be notified without undue delay and, where feasible, not later than 72 hours after the controller has become aware of the data breach. If the notification is not made within 72 hours, the explanation for the delay must be stated. The notification is sent by an electronic form at https://tietosuoja.fi/en/data-breach-notification. The supervisory authority

is responsible to without undue delay confirm that it has received the notification (controller's contact information can be found in the notification form).

3. High risk:

If a personal data breach will likely cause a high risk to the rights and freedoms of natural persons, in addition to the internal documentation and informing the authorities, the data subjects concerned must be informed directly and without undue delay.

Notification to the data subjects

If the personal data breach will likely cause a high risk to the rights and freedoms of natural persons, Oy Chemec Ab will inform also the data subjects about it as soon as possible. The communication shall be done personally via email or telephone and shall describe in clear and plain language the nature of the personal data breach, the likely consequences of it as well as any measures planned or done in order to mitigate its possible harmful effects.

Oy Chemec Ab will take all possible measures to ensure that the risks to the rights and freedoms of natural persons will not actualise or if they do, they will cause as little damage as possible.

If it seems likely that the data breach will result in criminal or civil action, the case will be reported to the police as soon as possible. The collection and storage of evidence will then be done according to the advice received from the relevant authorities.

After recovering from the data breach, a report will be made and used for improving the processing abilities and preparedness so that the recurrence of the breach can be prevented in the future.

8 RESPONSIBILITIES

Oy Chemec Ab's management is strongly committed to the procedures described in this data protection policy document. The CEO of is legally responsible for the activities under the GDPR in the organisation. The organisation's contact person in data protection related matters will manage and coordinate the actions stated in this document. He is also responsible for maintaining the data inventory as well as for giving instructions, communicating, and monitoring issues related to data protection.

All employees processing personal data will take part in the practical actions related to this data protection policy. Every employee is individually responsible for following the principles stated in this document and generally following the best practises related to data protection.

9 FOLLOW-UP

The core of the practical follow-up of issues related to data protection is the report composed by the organisation's contact person in data protection related matters. That report is annually presented to the steering group. The report will introduce the actions performed and planned in order to develop actions related to data processing. It will also provide a general view of the status related to personal data processing and data management in the organisation, including personal data breaches and their remedial actions.

All documentation related to data protection will be updated whenever necessary. The organisation's contact person in data protection related matters is responsible for reviewing and updating this data protection policy document whenever needed. The review of this data protection policy document belongs to the annual management review of organisation's quality system.

This document has been reviewed / updated on 17 June 2022.