Overview of Personal Data Processing for Employees (including individuals in a similar employment relationship)

according to Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the "GDPR Regulation") and Act No. 18/2018 Coll. on the protection of personal data and amending and supplementing certain Acts (hereinafter referred to as the "Data Protection Act").

The aim of this overview is to provide you with basic information about the processing of your personal data if you are performing work for us based on an employment contract or a similar employment relationship.

Complete information is available upon request at the Human Resources department.

Identification and contact details

The controller processing your personal data is Terichem Tervakoski, a. s., Štúrova 101, 059 21 Svit, ID: 31 705 472 (hereinafter referred to as the "Controller").

In case of any ambiguities, questions regarding the processing of your personal data, suggestions, or complaints if you believe that we process your personal data unlawfully or unfairly, or to exercise any of your rights, you can contact us at any time by sending an email to: gdpr@sk.tervakoskifilm.sk, or in writing to the address of the Controller.

Contact details of the Data Protection Officer supervising the processing of personal data: dpo3@proenergy.sk.

Basic overview of processing activities

We may process your personal data within the following processing activities (filling systems - FS):

Name and description of processing activity – purpose and legal basis, other important facts	Categories of data subjects	Categories of personal data	Retention period	Categories of recipients (external)
Human Resources and Payroll (HR&P) - we process your personal data for the purpose of managing personnel and payroll records, in compliance with legal obligations of the employer and obligations related to the employment contract or similar employment relationship, including pre-contractual relationships, contract negotiations, or with your voluntary consent, or in the exercise of the legitimate interests of the data controller or a third party in connection with: a. processing contact details for the purpose of fulfilling work duties and ensuring crisis management and business continuity management (FS 1.10, 1.11), b. sharing data within the corporate group for internal administrative purposes (primarily for maintaining internal records, contacting, collaborating, training, and approving compensation/benefits) (FS 1.22).	job applicants, employees, former employees (including individuals in a similar employment relationship), depending on the nature of the processing operation, personal data may also pertain to spouses of employees, dependent children of employees, parents of dependent children of employees, and close relatives.	the various HR&P agendas contain personal data (including sensitive personal data, particularly concerning health) that are relevant to the work the employee is expected to perform, is performing, or has performed.	For the duration necessary to fulfill the purpose, in accordance with the Archives and Records Management Act (but no longer than 70 years from the date of birth in the case of employee personal files).	(1) institutions and organizations, contractual partners, to whom processing is permitted by specific legal regulations, including government authorities and public bodies for the purpose of oversight and supervision, (2) processors, (4) contractual partners for whom provision is required to fulfill a contract between the data subjects and the data controller, (5) Personal data may, in certain cases, be shared based on legitimate interests, (3) If you have given us voluntary

				consent or instructed us to provide the data, your personal data may also be shared with other recipients.
Access control to the premises – authorized persons – if we have granted you regular access to our premises, we may monitor your authorization to enter, record your entry, and the entry of vehicles based on our legitimate interest.	employees, former employees (including agency staff), trainees, authorized external partners.	• personal data (standard – identification data, including photographs).	• Access and electronic card management – duration of the employment or similar relationship, contractual relationship, • entry records – 1 year.	(1) police, other authorized entity, (2) SBS.
Camera system – if you move within our monitored premises, which are marked at the entrance with a camera pictogram, you will be recorded on camera footage. The purpose of such recording is to ensure security (including crime detection), protect life, health, property, and the financial interests of the Controller, as well as to protect the life, health, and property of individuals present in the monitored area. We respect your right to privacy and do not monitor with cameras any zones where you may reasonably expect privacy – these are in particular areas designated for rest and relaxation (kitchen, toilets, changing rooms, lounge/relaxation room, dining tables). The recordings may be used to establish liability on your part in case of violations of internal regulations (provided you have been made aware of them) and/or legal regulations related to threats or damage to property, life, health, safety, or financial interests. The processing is based on the legitimate interest of the Controller or a third party.	persons moving within the monitored area.	• personal data (ordinary – captured on camera footage).	7 days.	(1,5) police, other authorized entity, (2) SBS.

Registry administration – we may process your personal data in accordance with a legal obligation for the purposes of managing the registry and recording mail. The processing of correspondence data may be carried out within the performance of a contractual relationship or a pre-contractual relationship (contract negotiations, contract performance, accounting management, handling complaints, etc.), in compliance with a legal obligation (e.g., reporting anti-social activities (whistleblowing), handling data subject requests, registry management), or within a legitimate interest (e.g., handling complaints, maintaining records of business partners, processing unexpected/unsolicited communications).	Natural persons – senders and recipients of correspondence.	• personal data (common identification data such as title, first name, last name, signature, address, e-mail address, phone number, or other data of varying sensitivity within the scope of communication under Act No. 305/2013 Coll., or voluntarily provided in the course of communication).	• maximum 10 years (registry), • retention of ordinary and official correspondence: 5 years.	(1) Ministry of Interior, other authorized entities, (2) archiving company, email storage provider.
Litigation – We may process your personal data if we are engaged in legal proceedings with you, based on a legal obligation and/or within the legitimate interest of the Controller or a third party, for the purpose of establishing, exercising, or defending legal claims.	natural persons – controllers and processors, authorized persons of controllers and processors, data subjects, other natural persons in the position of parties to the proceedings.	• personal data (especially identification, contact, and other personal data obtained or provided during legal proceedings). The sensitivity of the data is determined by the subject matter of the legal dispute (for example, data processing may involve information relating to the recognition of guilt for criminal offenses and misdemeanors).	10 years from the final conclusion of the legal proceedings.	(1a,5) courts, (1b,5) low enforcement authorities, (1c) other authorized entity.
Whistleblowing – we may process your personal data if you have submitted a non-anonymous report of a potential anti-social activity, or if you are the subject or participant in the investigation of a potential anti-social activity pursuant to a specific legal regulation.	natural persons who have submitted a report of anti-social activity or a request for protection when reporting serious anti-social activity (or their close persons for whom protection is requested) and natural persons who are investigated based on such a report.	• personal data – those provided in the report and data necessary for its review (especially, standard identification personal data of the reporter, persons involved in the violation, and details of the report, which may include data of varying sensitivity).	3 years (from the date of receipt of the report).	(1) The Slovakian Office for the Protection of Whistleblowers, participants in the proceedings, another competent administrative authority, the Prosecutor's Office of the Slovak Republic, courts of the Slovak Republic, other authorized entity.

Promotion – we may process your photographs, video recordings, and other information about you only to the extent and in the manner for which you have granted consent to the processing of personal data. If we have determined that consent is not required (redundant, requiring disproportionate effort, etc.) within the given purpose – for example, if you have participated or will participate in events organized by the controller for a wide audience – we may create and process photographs or other recordings as part of our legitimate interest. These data may be used for positive promotion, as well as for documentation and presentation purposes of the controller's activities. It is in our interest to document the controller's activities and present/promote them in the context of building good internal relations as well as external relations towards the controller and to maintain our good reputation. If you do not wish for your photographs, video recordings, or other related data to be used for documentation, presentation, or promotional purposes, you may exercise your rights (to object to processing or to withdraw consent) through the contacts provided at the beginning of this notice.	employees (including persons in a similar employment relationship), pupils, other natural persons.	• personal data (common—primarily identification data, captured in photographs, video/audio recordings, or other data related to expressions of a personal nature.	Duration of the employment relationship or until the purpose is fulfilled (5 years), does not apply to documents/records with permanent archival value in accordance with the Archives and Records Act.	(1) other authorized entity, (2) processor CHEMOSVIT, a. s.
Staff meals - we may process your personal data if you choose to use employee catering services, provided this arises from the performance of your employment contract or another agreement.	employees (including persons in a similar employment relationship, agency workers), students in professional training/dual education, external persons.	• personal data (common data related to the provision of meals – identification, financial information, meal selection).	5 years.	(2) meal provider, (1) other authorized entity.

Technical and organizational measures – in order to ensure your security as well as ours (including your personal data), to demonstrate compliance with our legal obligations, and to assert, exercise, or defend our legal claims or the claims of third parties, we may process records containing your personal data. These may include, for example: -records of your consent to data processing, -records of fulfillment of our information obligations towards you, -records of handling your requests, -records of authorized/assigned accesses and assets and their use, if we have granted/assigned them to you, -records necessary for investigating security incidents and data protection breaches, -records (confirmations) of training provided to you, -records of confidentiality commitments you have made, -records if you were part of our control activities or audits, -other records related to the implementation of adopted technical and organizational measures. Processing is carried out in the legitimate interest of the controller and also as an obligation arising from the GDPR. The records may be used to establish accountability towards you and as evidence for asserting, exercising, or defending the legal claims of the controller or a third party (especially in connection with threats or breaches to security, including the protection of human life and health, property, financial or material damage, interruption of operations, damage to reputation, leakage of know-how, etc.).	employees, data protection officer, applicants exercising their rights, persons towards whom the controller fulfills obligations arising from the GDPR, persons involved in or addressed in connection with a security incident, processors, other external entities (for example, persons consulted on the issue – consultants, auditors, lawyers), employees of authorities under specific legal regulations (e.g., employees of the supervisory authority in the context of consulting or control activities), etc.	• personal data (standard – identification, contact data, which, depending on the nature of the matter being addressed, may be supplemented with other necessary data of various types – e.g., login information, data related to user/offender behavior (e.g., login/logout logs, activities), data necessary to verify the identity of the person exercising their rights, data indicating breaches of internal regulations (e.g., circumventing security settings, etc.), and similar).	According to the chapter "Record Keeping and Archiving" of the Personal Data Protection Policy and the Information Security Policy (most records are kept for 3 years or less, records concerning deletions or containing contracts for 5 years, and some records permanently – e.g., those related to the handling of security incidents, impact assessments, notifications to data subjects, etc.).	(1a,5) data protection officer, supervisory authority of SR, (1b,5) police, the Prosecutor's Office of the Slovak Republic, courts of SR, (1c) other authorized authority.

Obligation to provide personal data,

The obligation to provide personal data varies for each of the processing activities mentioned above. In cases where the processing is based on your voluntary consent, you are not obliged to provide personal data.

However, by not providing them, for example, you may not be able to use our service that is based on consent, or you may not be able to benefit from it.

In cases where the processing is a legal or contractual requirement, or a task that we are obligated to perform in the public interest, you are required to provide us with personal data. Failure to do so may result in a breach of the law or hinder the use of our services, as we will not be able to fulfill our legal/contractual obligations.

The provision of personal data processed within our legitimate interest is mandatory, but you have the right to object to such processing. We will always properly assess your request, but it is possible that, in certain cases, we will not be able to comply with your request, and the provision of personal data will remain mandatory. Similarly, when we carry out profiling, you have the right to request that you are not included in it.

The transfer of personal data to a third country/international organization is not carried out.

Profiling is not carried out.

Additional information

Data from some of the above-mentioned processing operations may be used, where applicable and to the necessary extent, to prove, enforce, or defend our legal claims, or the legal claims of third parties (for example, providing data to law enforcement authorities, executors, lawyers, etc.), within judicial or extrajudicial proceedings, debt collection, etc. Some obtained personal data (e.g., confirmations, records, other documents confirming a particular fact, etc.) may be retained and used as "evidence" for audit purposes, third-party control activities, or for verifying the proper fulfillment of the Controller's obligations under legislative requirements or other requirements (contractual, sectoral, etc.).

Your rights

As a data subject whose personal data we process, you have the following rights under the GDPR Regulation and the Data Protection Act in connection with the processing of personal data: the right to request access to your personal data being processed, the right to correct (or supplement) personal data, the right to erasure or rectification personal data processing, the right to object to the processing of personal data, the right to the ineffectiveness of automated individual decision-making, including profiling, the right to data portability, the right to withdraw consent to the processing of personal data. If you decide to exercise any of your rights, you can use our request form available in the complete information on the processing of your personal data. If you are not satisfied with our response or believe that we have violated your rights or process your personal data unfairly or unlawfully, you have the right to file a complaint with the supervisory authority, which is the Authority of data protection of the Slovak Republic.