Personal Data Protection Policy

Rețele Electrice România S.A.
B-dul. Mircea Vodă 30, et. 3, Sector 3, București
Nr. de ordine în Registrul Comerțului J2002001859405, Cod Unic de înregistrare 14507322,
Capital social subscris și vărsat 580.355.660 lei
www.reteleelectrice.ro

Table of Contents

Rețele Electrice România S.A.
B-dul. Mircea Vodă 30, et. 3, Sector 3, București
Nr. de ordine în Registrul Comerțului J2002001859405, Cod Unic de înregistrare 14507322,
Capital social subscris și vărsat 580.355.660 lei
www.reteleelectrice.ro

Rețele Electrice România S.A.
B-dul. Mircea Vodă 30, et. 3, Sector 3, București
Nr. de ordine în Registrul Comerțului J2002001859405, Cod Unic de înregistrare 14507322,
Capital social subscris și vărsat 580.355.660 lei
www.reteleelectrice.ro

PART 1 – SCOPE, PURPOSE, ADOPTION & REVIEW OF THE POLICY

1.Scope & Purpose of the Policy

1.1. The Personal Data Protection Policy (hereinafter referred to as "Policy") sets the fundamental principles and rules governing the processing and protection of personal data processed by **RETELE ELECTRICE ROMANIA S.A.** (hereinafter "the "**Company**"), as well as the main roles and responsibilities for managing personal data protection issues and for overseeing the adequacy of the level of personal data protection within the Company.

1.2. The Policy applies to all personal data processing activities that fall within the scope of the Company's business activities.

1.3. The purpose of the Policy is to protect personal data in accordance with the applicable legislative and regulatory framework, to enhance the trust of interested parties (employees, shareholders, customers, potential customers, legal representatives, partners, and other third parties), and to safeguard the reputation and competitive position of the Company and the Group in the market.

1.4. The Policy applies to the members of the Board of Directors, persons who are part of the Company's administrative, management or supervisory bodies, as well as managers, employees and collaborators connected to the Company by contractual relationships of any type, also occasional and/or solely temporary.

1.5. In the event of a conflict between the obligations of this Policy and the provisions of the applicable personal data protection legislation, the requirements of the legislation shall prevail.

2. Adoption and Review of the Policy

2.1. The Policy shall enter into force upon its approval by the Board of Directors of the Company.

2.2. The Policy undergoes periodic reviews (at least biennially) and is revised, when necessary to ensure alignment with the prevailing legal and regulatory framework and the operational needs of the Company. Additionally, the Policy is subject to review when significant changes occur in the business activities, such as changes in the business practices of the Company, which necessitate or entail substantial modifications in personal data processing. Policy reviews shall be documented, including cases where no changes are required.

2.3. Specific policies, standards, and/or procedures developed to implement this Policy are approved by the General Manager of the Company.

2.4. The Policy is available for all the Company's personnel through internal communication tools and is also published on the Company's website.

PART 2 – PERSONAL DATA PROTECTION GOVERNANCE FRAMEWORK

3. Company Responsibility

3.1. The Company, in its capacity as Data Controller and/or Data Processor, bears full responsibility for compliance with the applicable legislative and regulatory framework for personal data protection, as well as with this Policy, and must be able to demonstrate its compliance at any time.

4. Obligation for Data Protection Officer appointment

4.1. The Company designates a Data Protection Officer when its operations involve personal data processing that, due to their nature, scope, and/or purposes, may pose a high risk to the rights and freedoms of data subjects. Such operations include, but are not limited to, the regular and systematic monitoring of data subjects on a large scale and the processing of special categories of personal data on a large scale or data relating to criminal convictions and offenses.

For assessing if processing takes place on a large scale, the following aspects are considered:

4.1.1. the number of data subjects involved, either as a specific number or as a percentage of the population,

4.1.2. the volume and range of data,

4.1.3. the duration or permanent nature of the processing,

4.1.4. the geographical extent of the processing.

4.2. The Company is obliged to provide the Data Protection Officer with the requisite financial and human resources necessary for the fulfillment of their duties.

5. Responsibilities of the Data Protection Officer

5.1. The Data Protection Officer appointed by the Company shall be involved by the Company in all matters related to personal data protection in a timely manner, without receiving instructions from the Company when performing their duties. The primary responsibilities of the Data Protection Officer designated by the Company include:

5.1.1. Informing and advising the Company on its obligations pursuant to the GDPR and the relevant legislative framework regarding personal data protection.

5.1.2. Monitoring the Company's compliance with the personal data protection legislative framework and internal data protection policies and conducting relevant audits.

5.1.3. Supporting the Division heads in developing and updating procedures related to personal data protection within their authority.

5.1.4. Assisting in the investigation of cases where data subjects file a complaint with the Data Protection Authority.

5.1.5. Being informed and assisting in the investigation of personal data breach incidents and notifying them to the competent Authorities and/or data subjects.

5.1.6. Conducting awareness-raising and training activities for staff involved in processing operations.

5.1.7. Providing advice and support regarding personal data protection impact assessments/legitimate interest assessments and monitoring the implementation of the established risk mitigation measures in accordance with this Policy.

5.1.8. Collaborating with the supervisory authority and acting as the point of contact on issues related to personal data processing, including providing consultations, as appropriate, on any pertinent issues.

5.1.9. Assisting the Company in implementing the personal data protection strategy of PPC Group.

5.1.10. Assisting the Company with the integration and adaptation of PPC Group's data protection policies and standards into the Company's processes and operations, advising on the alignment with the broader compliance framework of the PPC Group.

5.1.11. Collaborating with the Company's Cyber Security Officer on issues concerning security in processing operations (e.g., designing technical and organizational measures, managing personal data breach incidents).

5.1.12. Providing ongoing support and guidance on data protection matters, including analyzing data processing activities and advising on compliance requirements, upon request from the Division heads.

6. PPC Group Data Protection Officer (Group DPO)

6.1 The PPC Group Data Protection Officer serves as the Data Protection Officer for PPC and the Group companies that are required to appoint a DPO and have not

independently appointed one, unless the provision of these services conflicts with the requirements of the applicable legislation or regulatory framework or if there are other operational reasons.

6.2. The Group Data Protection Officer develops Group-wide data protection policies and standards, aiming for uniform and consistent compliance of all Group companies with the applicable regulatory and legal framework, as well as the effective utilisation of compliance tools for monitoring, documenting, and automating relevant processes.

6.3. The Group Data Protection Officer determines the mechanisms for overseeing the level of personal data protection within PPC and the Group companies. The oversight mechanisms may include the establishment of key performance indicators (KPIs) as well as self-assessment procedures for each Group company.

6.4. Provided it is not prohibited by applicable legislation, the Group Data Protection Officer may carry out scheduled and/or ad hoc audits in the Group companies. These audits may be conducted by company personnel and/or external partners.

6.5. The Company must provide the Group Data Protection Officer with any information necessary for supervising the adequacy of the level of personal data protection in the PPC Group and must take appropriate measures to address any deficiencies identified. The Group Data Protection Officer monitors the implementation of these measures.

6.6. The Group Data Protection Officer annually informs the Group Audit Committee about the Group Companies' compliance program with personal data protection legislation.

7. Responsibilities of the Division Heads

7.1. The Division heads who hold responsibility for data processing activities, shall bear operational responsibility for compliance with data protection legislation and monitoring adherence to this Policy. Indicatively, they are responsible for:

7.1.1. Informing the Data Protection Officer at an early stage regarding new or amended personal data processing activities, whether arising from strategic planning and/or urgent operational requirements, in order to ensure that any personal data protection issues are examined and assessed.

7.1.2. Ensuring that the staff under their supervision is appropriately trained and informed in data protection matters.

7.1.3. Ensuring execution of personal data processing agreements according to paragraph 27 of this Policy and supervising data processors regarding the adherence to data protection obligations set within the said data processing agreements (e.g., following instructions and implementing technical and organizational measures for processing security).

7.1.4. Maintaining an up-to-date record of processing activities for which they are responsible, in accordance with paragraphs 18.2 and 18.3.

7.1.5. Ensuring compliance with personal data processing principles as defined by the legislation and this Policy, as well as with the recommendations issued by the Data Protection Officer.

7.1.6. Ensuring that a personal data protection impact assessment is conducted when required, prior to the commencement of processing and in collaboration with the Data Protection Officer, according to paragraph 29.

7.1.7. Implementing appropriate organizational and/or technical measures for personal data protection and ensuring compliance with obligations arising from the Company's Cybersecurity framework.

Such measures shall indicatively include access control, pseudonymisation or encryption, ensuring availability and integrity of systems, as well as the ability to detect and respond promptly to incidents of data breaches.

7.1.8. Responding to requests for the provision of information in the context of investigations or other actions carried out by the competent supervisory Authorities.

8. Employee's Obligations

8.1. All employees and service providers to the Company, irrespective of their employment status, are mandated to adhere to the legal framework governing personal data protection and the relevant rules as delineated in this Policy. They are also required to actively contribute to maintaining the requisite level of protection and security of personal data.

8.2. Employees shall receive and must attend training on the fundamental principles of personal data protection at least biennially. Participation in this training is compulsory.

8.3. Any violation of this Policy may result in consequences as stipulated in applicable legislation and the Company's regulatory framework.

PART 3 - CORE PRINCIPLES OF PERSONAL DATA PROCESSING

9. Purpose Limitation

9.1. Personal data are collected for specified, explicit, and legitimate purposes and are not further processed in a manner incompatible with those purposes ("purpose limitation").

9.2. Prior to any further processing for a different purpose, the following criteria are considered:

9.2.1. Any correlation between the purposes for which the personal data were collected and the purposes of the intended further processing,

9.2.2. The context in which the personal data have been collected, particularly with regard to the relationship between the data subjects and the Company in its role as data controller,

9.2.3. The nature of the personal data, especially concerning special categories of personal data,

92.4. The potential consequences of the intended further processing for the data subjects,

9.2.5. The presence of appropriate safeguards, which may include encryption or pseudonymization.

10. Data Minimization

10.1. The Company shall process personal data only when they are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ("data minimization principle").

10.2. When designing new systems, services, or processes involving the processing of personal data, the principle of data minimization is applied from the design stage. Only the personal data strictly necessary for the defined purpose are collected.

11. Data Accuracy

11.1. The Company shall take measures to ensure that personal data are accurate and, where necessary, kept up to date ("accuracy").

11.2. If the personal data are inaccurate with respect to the purposes of processing, the Company takes steps for their immediate deletion or correction.

12. Storage Limitation

12.1. The Company shall take measures to ensure that personal data are kept in a form that permits the identification of data subjects only for the time necessary for the purposes of personal data processing ("storage limitation").

12.2. When the purpose for processing personal data has been achieved, the personal data must be deleted or anonymized, unless otherwise specified in the applicable legal framework.

12.3. The retention period for personal data shall be defined based on the purposes for which the data is processed and any applicable legal or regulatory requirement, or documented business need. The retention period must be justified accordingly.

12.4. The prescribed retention periods are documented in the record of processing activities of the Company, in accordance with Article 30 of the GDPR, when available or provided by the Division.

13. Fairness in Processing

13.1. Personal data processing shall be conducted in accordance with the principle of fairness, ensuring that each processing activity is equitable, impartial, and just towards data subjects.

13.2. The Company is committed to maintaining practices that promote transparent and fair treatment of all data subjects, without discrimination or bias, regardless of gender, age, nationality, religion, political beliefs, or other characteristics.

13.3. Fairness shall be ensured both in the design of processing procedures and their implementation, avoiding practices that result in unfair or disproportionate outcomes to the detriment of the data subjects.

14. Lawfulness of Personal Data Processing

14.1. The processing of personal data is lawful only if and to the extent that at least one of the following conditions is met:

14.1.1. The data subject has given consent to the processing of their personal data for one or more specific purposes (GDPR, Art. 6.1(a)).

14.1.2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (GDPR, Art. 6.1(b)).

14.1.3. Processing is necessary for compliance with a legal obligation to which the controller is subject (GDPR, Art. 6.1(c)).

14.1.4. Processing is necessary to protect the vital interests of the data subject or another natural person (GDPR, Art. 6.1(d)).

14.1.5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller (GDPR, Art. 6.1(e)).

14.1.6. Processing is necessary for the purposes of the legitimate interests pursued by the Company as the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, especially if the data subject is a child (GDPR, Art. 6.1(f)).

14.2. Processing of special categories of personal data is prohibited, unless:

14.2.1. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes (GDPR, Art. 9.2(a)).

14.2.2. Processing is necessary for the performance of obligations and the exercise of specific rights of the Company, as the data controller or of the data subject in the

field of employment and social security and social protection law, in so far as it is authorized by national law or a collective agreement pursuant to national law providing for appropriate safeguards for the fundamental rights and interests of the data subject (GDPR, Art. 9.2(b)).

14.2.3. Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of providing consent (GDPR, Art. 9.2(c)).

14.2.4. Processing relates to personal data which have been manifestly made public by the data subject (GDPR, Art. 9.2(e)).

14.2.5. Processing is necessary for the establishment, exercise, or defense of legal claims (GDPR, Art. 9.2(f)).

14.2.6. Processing is necessary for reasons of substantial public interest, based on Union or Member State law, provided that it is proportionate to the objective pursued, respects the essence of the right to personal data protection, and includes appropriate and specific measures to safeguard the fundamental rights and interests of the data subject (GDPR, Art. 9.2(g)).

14.2.7. Processing is necessary for the purposes of preventive or occupational medicine, the assessment of employees' working capacity, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional (GDPR, Art. 9.2(h)).

14.2.8. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Union or Member State law, which shall be proportionate to the objective pursued, respect the essence of the right to personal data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject (GDPR, Art. 9.2(i)).

15. Data Subject consent

15.1. When processing is predicated on the consent of the data subject, the Company must be able to demonstrate that the data subject has provided consent for the processing activity.

15.2. If the data subject's consent is given within the context of a written declaration that also pertains to other matters, the request for consent must be presented in a manner that is clearly distinguishable from the other matters, in an understandable and easily accessible form, using clear and plain language.

15.3. Consent must be given by a clear affirmative act that indicates a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data relating to them, for instance by a written statement, including by electronic means (e.g., ticking a box when visiting a website), or by an oral statement.

15.4. When processing has multiple purposes, consent must be given for all of them.

15.5. If the data subject's consent is to be obtained by electronic means, the request for consent must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.

15.6. The data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

15.7. Prior to providing consent, the data subject is informed at least about the purpose of personal data processing and the identity of the Company.

15.8. Withdrawal of consent is as easy as providing it.

15.9. In assessing whether consent is freely given, utmost account is taken of whether, among others, the execution of a contract, including the provision of a service, is made

conditional on consent to the processing of personal data that is not necessary for the execution of that contract.

15.10. To ensure that consent is freely given, consent should not form a valid legal basis where there is a clear imbalance between the data subject and the data controller.

15.11. Evidence of consent must be easily accessible and available in order to respond to the exercise of data subjects' rights and prove compliance.

16. Information Regarding Personal Data Processing

16.1. The Company, as data controller, must provide the data subject with the following information:

16.1.1. The identity and contact details of the Company.

16.1.2. The contact details of the Data Protection Officer or the Group DPO, if the case.

16.1.3. The purposes of processing for which the personal data are intended as well as the legal basis for the processing.

16.1.4. The source from which the personal data originate, and, if applicable, whether they originate from publicly accessible sources, in cases where the data have not been obtained directly from the data subject.

16.1.5. If the processing is based on the legal basis of legitimate interests, description of the legitimate interests pursued by the controller or by a third party.

16.1.6. The recipients, or the categories of recipients of personal data, if any.

16.1.7. Where applicable, information about transfers of personal data outside the European Economic Area.

16.1.8. The period for which the personal data will be stored, or, when that is not possible, the criteria used to determine that period.

16.1.9. The right to request from the Company access to, correction or erasure of personal data, or restriction of processing relating to the data subject, or object to processing, as well as the right to personal data portability.

16.1.10. In cases where processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

16.1.11. The right to lodge a complaint with the supervisory authority.

16.1.12. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data.

16.1.13. The use of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

16.2. When the Company intends to further process personal data for a purpose other than that for which they were collected, the Company shall provide the data subject, prior to that further processing, with information on that other purpose with any other necessary information, as referred to in paragraph 16.1.

17. Automated Decision-Making, Including Profiling

17.1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects for them or similarly significantly affects them.

17.2. Exceptionally, automated decision-making that produces legal effects or significantly affects the data subject is permitted when the decision:

17.2.1. Is necessary for entering into, or performance of, a contract between the data subject and the Company,

17.2.2. Is authorized by law, or

17.2.3. Is based on the explicit consent of the data subject.

17.3. In the above cases, the Company shall implement suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests, including the right to obtain human intervention on the part of the Company, to express their point of view, and to contest the decision.

17.4. The Company shall ensure fair and transparent processing, providing meaningful information about the logic involved, as well as the significance and the envisaged consequences of processing.

17.5. Automated decision making or profiling, should not concern children, nor should they be based on special categories of personal data, unless, in the latter case, the Company has the explicit consent of the data subject.

18. Record of Processing Activities

18.1. The Company keeps a comprehensive record of all processing activities it undertakes in accordance with art. 30 GDPR.

18.2. For activities where the Company acts as a data controller, the record includes:

18.2.1. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the Data Protection Officer or the Group DPO, if the case.

18.2.2. The purposes of the personal data processing.

18.2.3. A description of the categories of data subjects and the categories of personal data.

18.2.4. The categories of recipients, including recipients in third countries.

18.2.5. Where applicable, transfers of personal data to a third country, including identification of said third country and documentation of appropriate safeguards.

18.2.6. Where possible, the envisaged time limits for erasure of the different categories of personal data.

18.2.7. Where possible, a general description of the technical and organizational security measures.

18.3. For activities where the Company acts as a data processor, the record includes:

18.3.1. The name and contact details of the Company, and the data controllers on whose behalf it acts, as well as the Data Protection Officer.

18.3.2. The categories of processing activities carried out on behalf of each data controller.

18.3.3. Where applicable, transfers of personal data to a third country, including identification of said third country and documentation of appropriate safeguards.

18.3.4. Where possible, a general description of the technical and organizational security measures.

18.4. The record of processing activities is updated when changes in processing activities occur, while its accuracy and completeness are periodically reviewed by the Division Heads.

PART 4 – DATA SUBJECT RIGHTS

19. Right to Access (Article 15 GDPR)

19.1. Data subjects have the right to access the information referenced in paragraph 16 of this Policy.

19.2. The related information should be made available to the data subject in a comprehensible format and within a reasonable time frame. This is generally achieved through printed or electronic communication.

19.3. In any case, the data subject should be informed within one month from the receipt of the request. This period may be extended by two additional months where necessary, considering the complexity and number of requests. The data subject should be informed of any such extension.

19.4. The Company provides a copy of the personal data undergoing processing. For any additional copies requested by the data subject, the Company may charge a reasonable fee for administrative costs.

20. Right to Rectification (Article 16 GDPR)

20.1. The data subject has the right to request the rectification of inaccurate personal data, or the completion of incomplete personal data concerning them.

21. Right to Erasure (Article 17 GDPR)

21.1. The data subject may request the erasure of personal data, particularly when the data is no longer necessary, when the data subject withdraws consent, or objects to the processing.

21.2. Erasure does not apply in cases where processing is necessary for compliance with a legal obligation that requires processing, or for the establishment, exercise, or defense of legal claims.

22.Right to Restriction of Processing (Article 18 GDPR)

22.1. The data subject may request the restriction of processing mainly when:

22.1.1. The accuracy of personal data is contested by the data subject, for a time period allowing the Company to verify the accuracy of the personal data,

22.1.2. The processing is unlawful, and the data subject opposes to the erasure of personal data and requests the restriction of their use instead,

22.1.3. The Company no longer needs the personal data for the purposes of processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims,

22.1.4. The data subject has objected to the processing, while the verification of whether the legitimate grounds of the controller override those of the data subject remains pending.

23. Right to Object (Article 21 GDPR)

23.1. The data subject has the right to object, at any time and on grounds relating to their particular situation, to the processing of their personal data, which is based on legitimate interests.

23.2. The Company shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

23.3. If personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of their personal data for the specific marketing purposes, which may include profiling to the extent that it is related to such direct marketing.

23.4. When data subjects object to the processing for direct marketing purposes, their personal data shall no longer be processed for such purposes.

24. Right to Personal Data Portability (Article 20 GDPR)

24.1. The data subject has the right to receive the personal data concerning them, which they have provided to the data controller, in a structured, commonly used, and

machine-readable format, when processing is based on consent or a contract and carried out by automated means.

24.2. In exercising the right to personal data portability pursuant to paragraph 24.1, the data subject has the right to have personal data transmitted directly from one controller to another, where technically feasible.

25.Right to Withdraw Consent (Article 7 GDPR)

25.1. When processing is based on the data subject's consent, they retain the right to withdraw it at any time, without affecting previous processing based on consent.

25.2. The data subject has the right to object at any time to the use of their personal data if such data are used for purposes not mandated by law.

25.3. The right to object applies even if the data subject had previously given consent for the use of their personal data.

26. Exercising Data Subject Rights

26.1. The Company manages data subjects' requests following specific procedures.

26.2. The Company responds to data subjects' requests without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months where necessary, considering the complexity of the request and the number of requests made.

26.3. In case of a delay, the Company informs the data subject of the extension within one month from the receipt of the request, along with the reasons for the delay.

26.4. If the data subject submits the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

26.5. The Company uses all reasonable measures to verify the identity of a data subject requesting access, retaining identification data only for the time needed. The Company must not retain personal data solely for the purpose of responding to potential future data subject requests.

26.6. The Company reserves the right to refuse, wholly or partially, a data subject's request only when it falls under a GDPR exception or a national law provision. In any case, the data subject is informed in writing and with reasoning about the decision not to satisfy their request, as well as about their right to file a complaint with the Data Protection Authority (DPA).

PART 5 – PERSONAL DATA PROCESSING ASSIGNMENT AND PERSONAL DATA TRANSFERS OUTSIDE THE EEA

27. Due Diligence and Contractual Requirements

27.1. Whenever the Company assigns personal data processing to a processor or undertakes personal data processing on behalf of a controller or jointly processes personal data with another controller, it must demonstrate due diligence in regulating the lawful and fair processing of personal data before concluding the corresponding agreement.

27.2. The Company shall only use data processors who provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing meets the requirements of the GDPR and ensures the protection of the rights of the data subjects.

27.3. The engagement of a data processor shall be governed by a data processing agreement, which is legally binding on the processor with respect to the Company acting as data controller and clearly sets forth the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and

categories of data subjects involved, as well as the rights and obligations of the Company. In particular, the agreement shall stipulate that the data processor:

27.3.1. Processes personal data solely on documented instructions from the Company, including instructions regarding transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject. In such cases, the processor shall inform the Company of the legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

27.3.2. Ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

27.3.3. Takes all necessary technical and organizational measures.

27.3.4. Does not engage another processor without prior specific or general written authorization from the Company. In the case of general written authorization, the processor informs the Company of any intended changes regarding the addition or replacement of other processors, thereby giving the Company the opportunity to object to such changes.

27.3.5. When the processor engages another processor for carrying out specific processing activities on behalf of the Company, the same personal data protection obligations as set out in the agreement between the Company and the processor are imposed on that other processor by way of a contract, in particular, providing sufficient guarantees to implement appropriate technical and organizational measures so that processing will meet the requirements of the GDPR.

27.3.6. Takes account of the nature of the processing and assists the Company by appropriate technical and organizational measures, insofar as this is possible, for fulfilling the Company's obligation to respond to requests for exercising the data subject's rights.

27.3.7. Assists the Company in ensuring compliance with obligations regarding the security of processing, management of personal data breach incidents, and conducting impact assessments, considering the nature of processing and the information available to the processor.

27.3.8. At the choice of the Company, deletes or returns all personal data to the Company after the end of the provision of processing services and deletes existing copies, unless Union or Member State law requires the storage of the personal data.

27.3.9. Makes available to the controller all information necessary to demonstrate compliance with the obligations set forth and allows for and contributes to audits, including inspections, conducted by the Company or another auditor mandated by the Company.

27.4. The Company must implement appropriate monitoring mechanisms to ensure that services provided by processors are in compliance with the obligations set out in the agreed contracts.

27.5. In cases where the Company acts as a joint controller with another legal entity, an agreement must be made between the parties, transparently setting out their respective responsibilities for compliance with GDPR obligations, particularly regarding the exercise of the data subjects' rights and corresponding duties to provide information to data subjects. The agreement may specify a point of contact for data subjects.

28. Personal Data Transfers Outside the EEA

28.1. Any transfer of personal data to a country outside the European Economic Area (EEA)[1] or to an international organization shall only occur only if the conditions set forth

[1] EU Countries, Iceland, Norway and Liechtenstein

in the GDPR are met, ensuring that the level of protection of natural persons guaranteed by the GDPR is not undermined.

28.2. Personal Data transfer outside the EEA may occur under the following circumstances:

28.2.1. The European Commission has issued an Adequacy Decision confirming that the level of personal data protection in a country outside the EEA or in an international organization is essentially equivalent to that in the European Economic Area.

28.2.2. Appropriate safeguards are provided regarding the recipient organization according to Article 46 of the GDPR (e.g., EU standard contractual clauses, binding corporate rules), while simultaneously, the legal entity acting as the exporter conducts a Transfer Impact Assessment to determine whether the legislation or practices of the non-EEA country prevent the effectiveness of the appropriate safeguards (for example, due to legislation compelling access to personal data). If the assessment indicates that third-country laws or practices affect the effectiveness of the transfer tool, then the transfer can occur only if the exporter establishes additional measures to ensure that the level of protection of the transferred personal data approaches the EU standard of substantive equivalence.

28.2.3. The transfer takes place based on one of the derogations provided in Article 49 of the GDPR as follows:

a) the data subject has expressly consented to the proposed transfer, having been informed of the potential risks that such transfers pose to the data subject rights in the absence of an adequacy decision and appropriate safeguards,

b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject,

c) the transfer is necessary for the conclusion or performance of a contract concluded for the benefit of the data subject between the data controller and another natural or legal person,

(d) the transfer is necessary for important reasons of public interest,

(e) the transfer is necessary for the establishment, exercise or defence of legal claims,

(f) the transfer is necessary to protect the vital interests of the data subject or of other persons where the data subject lacks the physical or legal capacity to give consent,

(g) the transfer is carried out from a registry which, in accordance with EU or State Member State law, is intended to provide information to the public and is open for consultation either by the general public or by any person who can rely on a legitimate interest, but only if the conditions laid down in Union or Member State law are met in each case.

PART 6 – DATA PROTECTION BY DESIGN & PROCESSING SECURITY

29. Data Protection Impact Assessment (DPIA)

29.1. When a type of processing, particularly with the use of new technologies, considering the nature, scope, context, and purposes of processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall conduct, prior to processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

29.2. An assessment may cover a set of similar processing operations that present similarly high risks.

29.3. A Data Protection Impact Assessment is required in particular in cases of:

29.3.1. Systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

29.3.2. Large-scale processing of special categories of data or personal data relating to criminal convictions and offenses.

29.3.3. Systematic monitoring of a publicly accessible area on a large scale.

29.3.4. Any processing operation included in the list established by the competent Data Protection Authority regarding the types of processing operations subject to the requirement for a DPIA.

29.4. The assessment contains at least:

29.4.1. A systematic description of the envisaged processing operations and the purposes of processing, including, where applicable, the legitimate interests pursued by the Company.

29.4.2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes.

29.4.3. An assessment of the risks to the rights and freedoms of data subjects.

29.4.4. The envisaged measures to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the legislative framework, taking into account the rights and legitimate interests of data subjects and other stakeholders.

29.5. The DPIA is conducted under the authority of the Division Head responsible for overseeing the relevant processing activities. When conducting a DPIA, the opinion of the Data Protection Officer is sought regarding:

29.5.1. Whether or not a DPIA is required for the personal data processing.

29.5.2. Which methodology should be followed for conducting the DPIA.

29.5.3. Whether the DPIA will be conducted internally or it shall be outsourced to an external partner. In the case of outsourcing, the external party selection is done with the approval of the Data Protection Officer or the Group DPO, as the case may be.

29.5.4. The type of safeguards (including technical and organizational measures) the Company should apply in order to mitigate risks to the rights and interests of data subjects.

29.5.5. Whether the DPIA was correctly conducted and whether its conclusions (regarding whether or not to proceed with the processing and what safeguards to implement) are consistent with relevant legislation.

29.6. If the DPIA indicates that the processing operation would result in a high residual risk, the Company must, according to Article 36 GDPR, consult the competent supervisory authority prior to processing.

30. Security of processing

30.1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company implements appropriate technical and organizational measures to ensure an appropriate level of protection of personal data against risks.

30.2. When assessing the appropriate level of security, particular consideration is given to the risks presented by processing, particularly from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

30.3. Measures should include, but are not limited to:

30.3.1. Measures to prevent unauthorized individuals from accessing personal data processing systems.

30.3.2. Measures to ensure that authorized persons for personal data processing systems have access only to personal data they are authorized to handle.

30.3.3. Measures to ensure that personal data cannot be read, copied, altered, or deleted by unauthorized persons during processing (e.g., encryption or pseudonymization).

30.3.4. Measures to ensure that personal data processed by third parties/processors are processed only in accordance with the instructions of the controller.

30.3.5. Measures to ensure that personal data are protected against accidental destruction or loss (e.g., backups, system recovery plans, etc.).

30.3.6. Measures to ensure that personal data collected for different purposes are processed separately.

30.4. Additionally, the Company applies appropriate technical and organizational measures to ensure that, by default, only personal data necessary for each specific purpose of processing are processed. This obligation applies to the amount of personal data collected, the extent of processing, the storage period, and their accessibility. Specifically, these measures ensure that, by default, personal data are not made accessible without personal intervention to an indefinite number of persons.

31.Personal Data Breach

31.1. The Company must be able to assess the risk arising from a personal data breach incident concerning the rights and freedoms of natural persons. Within this context, it must have procedures for timely and effective identification and management of data breach incidents.

31.2. When assessing the risk of an incident to the data subject's rights and freedoms, the specific circumstances of the breach are examined, including its severity and potential impacts. The assessment must particularly consider the following criteria:

31.2.1. Type of breach.

31.2.2. Nature, sensitivity, and volume of affected personal data.

31.2.3. Degree of identifiability of the data subject.

31.2.4. Severity of consequences for the data subject.

31.2.5. Special characteristics of the data subject.

31.2.6. Number of data subjects affected.

32. Notification of Personal Data Breaches

32.1. In the event of a personal data breach, the Company, acting as Controller, must notify the relevant supervisory authorities according to the GDPR and national law.

32.2. When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the Company must promptly notify the data subject of the personal data breach.

32.3. If the Company is acting as a processor, it shall notify the controller without undue delay after becoming aware of a personal data breach.

33. Documentation of Personal Data Breaches

33.1. The Company maintains an appropriate record of personal data breach incidents.

33.2. This record includes all details regarding the incident (date, actions, involved parties, action plan, etc.) as well as details about its assessment and the notification to supervisory authorities and/or data subjects.

DEFINITIONS:

Controller

The legal or natural person or other entity that determines the purposes and means of processing personal data and assigns the personal data processing to the Company.

Consent of the Data Subject

Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Subject

An identified or identifiable natural person to whom the data refers to.

Encryption

The process of converting personal data from its original form into a coded form that can only be read by those who possess the appropriate cryptographic key to decrypt it.

Joint Controller

The natural or legal person who, along side with the Controller, determines the purposes and means of processing personal data.

Personal Data

Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Processing of Personal Data

Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Processor

The legal or natural person or other entity that processes personal data on behalf of the Controller.

Profiling

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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Pseudonymization

Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Recipient

A natural or legal person, public authority, agency or another body to which personal data are disclosed, whether it is a third party or not.

Special Categories of Personal Data

These are personal data related to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation of a natural person

Supervisory Authority

An independent public authority established by a Member State responsible for monitoring the application of personal data protection law in order to protect the fundamental rights and freedoms of data subjects concerning processing and to facilitate the free flow of personal data within the Union.

Third Party

A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

This Policy shall enter into force upon its approval by the Board of Directors of the Company, respectively on 29.10.2025.