Data protection policy in the company

VanKing Celkar Group Simple Joint Stock Company

Pursuant to Article 24 of Regulation 2016/679, as of 25.05.2018, the Data Protection Policy is introduced

Table of contents

1. General provisions

1. This document entitled "Data Protection Policy" (hereinafter referred to as the "Policy") is intended to map the requirements, principles, regulations for the protection of personal data at the Entity.
2. This Policy is a data protection policy within the meaning of the RODO - 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.EU.L.2016.119.1.
3. The Policy, which sets out the principles of data processing and data protection at the Entity, includes in particular:

- description of the Entity's data protection rules,
- references to specific annexes (model procedures or instructions for specific areas of data protection requiring clarification in separate documents).

2. Definitions

Whenever the Policy refers to:

1. Personal Data Administrator (ADO)/Entity - VanKing Celkar Group Simple Joint Stock Company with registered office in Niepołomice, Podłęska 25, 32-005 Niepołomice, entered into the Register of Entrepreneurs kept by the District Court for Kraków - Śródmieście in Kraków, 12th Commercial Department, under KRS number 0001045488, NIP 6792691789, REGON 356291869;
2. Instruction - shall mean the Instruction which defines the manner of management of the computer system used for the processing of personal data, which has been adopted by the ADO as a binding document in the Entity;
3. Regulation (RODO) - means 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.EU.2016.119.1 of 2016.05.04;
4. personal data - means information about 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 the natural person;
5. special categories of data - means the personal data listed in Article 9(1) of the RODO, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning the health, sexuality or sexual orientation of that person;

6. criminal data - data listed in Article 10(1) of the RODO, i.e. data on criminal convictions and offences
7. password - means a sequence of letter, digital or other characters, known only to the user, giving him/her access to personal data processed in a computer system,
8. identifier - shall mean a sequence of letter, digital or other characters uniquely identifying a person authorised to process personal data in a computer system,
9. data integrity - means the property of ensuring that personal data have not been altered or destroyed in an unauthorised manner,
10. system integrity - means the property ensuring the integrity of the system, the impossibility of any unauthorised modification,
11. data carrier - means a medium used for recording and storing information, e.g. pendrives, discs, hard disks,
12. person - means the data subject, unless the context clearly indicates otherwise;
13. recipients of the data - shall mean the natural or legal person, public authority, individual or any other body to whom personal data are disclosed, whether or not a third party. However, public authorities which may receive personal data in the context of a specific proceeding in accordance with Union or Member State law are not considered recipients; the processing of such data by these public authorities must comply with the data protection legislation applicable according to the purposes of the processing;
14. Confidentiality of data - means the property ensuring that data is not disclosed to unauthorised parties,
15. entrusting the processing of personal data - shall mean ordering the performance of personal data processing activities by the processor for the benefit of ADO on the basis of an appropriate provision in the agreement ensuring personal data security conditions in accordance with the provisions of the Act and the Regulation or on the basis of a separate written agreement on entrusting the processing of personal data concluded pursuant to Art. 28 RODO,
16. Processor - means a person or organisation to whom the Subject has entrusted the processing of personal data,
17. personnel - it shall be understood as persons providing work for the benefit of ADO on the basis of employment relationship, civil law contracts (e.g. contract to perform a specific task or contract of mandate), entrepreneurs performing their activities personally and on their own, trainees, interns, persons directed to work under contracts with temporary work agencies performing work related to personal data processing within the structures of ADO;
18. RCPD or Register - means the Register of Data Processing Activities
19. Person authorised to process personal data - shall mean a member of staff to whom the ADO has given a named authorisation in writing to process data at the Entity,
20. User - means an authorised person to whom ADO has given an ID and assigned a password,
21. data processing - an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

22. Accountability - means the property ensuring that the actions of an entity can be clearly attributed only to that entity,
23. Computer system of the Personal Data Controller - means computer hardware, software, data operated in a set of cooperating devices, programs, information processing rules and software tools used for data processing,
24. sharing of personal data - means the communication, disclosure, dissemination of personal data to the data recipient,
25. erasure - means the destruction of personal data or their modification in such a way that the identity of the data subject cannot be established,
26. Pseudonymisation - means the processing of personal data in such a way that they 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 covered by technical and organisational measures which make it impossible to attribute it to an identified or identifiable natural person;
27. Authentication - means the action of verifying the declared identity of a natural person or entity,
28. IT system security - means the implementation of appropriate administrative, technical and physical measures to secure the technical resources and to protect against modification, destruction, unauthorised access and disclosure or acquisition or loss of personal data,
29. collection of personal data - means the collection of data from the data subject or from other sources,
30. personal data filing system - shall mean an organised set of personal data which are accessible according to specific criteria, whether that set is centralised, decentralised or dispersed on a functional or geographical basis,
31. Data subject's consent - means a freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, either by a declaration or by a clear affirmative action, consents to the processing of personal data concerning him or her.

3. Purpose of the Policy, scope, amendments and updates

1. The Personal Data Controller, attaching particular importance to the protection of personal data processed in the structures of the Entity, declares to take all possible measures necessary to prevent data security risks resulting from events such as:
   a) breach of data security by unauthorised processing,
   b) disclosure to unauthorised persons of the data protection rules applicable by ADO,
   c) Intentional or accidental dispersion of data on the Internet by circumventing the system's security measures or taking advantage of the ADO's IT system errors,
   d) the unforeseen impact of external factors on IT system resources, such as fire, flooding of premises, building disaster, robbery, theft, burglary, terrorist activities,
   e) inappropriate environmental parameters that interfere with the operation of computer equipment (excessive humidity or very high temperatures, electromagnetic field effects and others),
   f) hardware or software failures that clearly indicate deliberate breaches of data protection, malfunctioning of maintenance procedures, including condoning the repair of equipment containing personal data outside the premises of the ADO,
   g) attacks from the internet,
   h) breaches of the principles set out in the data protection documentation by authorised persons related to their failure to comply with data protection rules, including in particular:
   i) leaving work or leaving the workplace contrary to procedures,
   j) disclosure to unauthorised persons of the data protection principles applied at ADO.
2. The ADO develops, approves and ensures the implementation of the Policy as an expression of his/her will to implement the law on the protection of personal data and to ensure the protection of the personal data of which he/she is the controller from all kinds of internal and external threats, whether conscious or unconscious.
3. Independently of the Policy, a Management Manual for the IT system used to process personal data has been developed and implemented.
4. The protection of personal data is implemented through: physical safeguards, organisational procedures, system software, applications and through the behaviour of authorised persons.
5. The safeguards indicated above are intended to ensure the confidentiality, integrity and accountability of the personal data processed by the ADO, as well as the integrity of the IT system through which this processing is carried out.
6. Where the provisions of any laws provide for more far-reaching protection of personal data than the Regulation, the provisions of those laws shall apply.
7. The rules set out by the Policy apply to everyone:
   a) of personal data processed at the Entity, both in the case where it is the controller and in the situation where it processes the data entrusted on the basis of contracts concluded pursuant to Article 28 of the Regulation,
   b) storage media, e.g. paper, magnetic, optical, etc., on which personal data is or will be stored,
   c) location - the buildings and premises at the disposal of the Subject where personal data are or will be processed,

d) persons constituting staff and other persons with access to personal data.

4.Data protection in the Entity - general principles

1. Pillars of data protection in the Entity:
2. Legality - The controller is committed to protecting privacy and processes data in accordance with the law,
3. Security - The ADO ensures an adequate level of data security by taking continuous measures in this regard,
4. Individual rights - ADO enables individuals to exercise their rights and realises those rights,
5. Accountability - the ADO shall document how it complies with its obligations in order to be able to demonstrate compliance at any time
6. Data protection principles:
7. Personal data is:
    a) processed lawfully, fairly and in a manner transparent to the data subject ('lawfulness, fairness and transparency');
    b) collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes ("purpose limitation");
    c) adequate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimisation");
    d) correct and updated as necessary; every reasonable step must be taken to ensure that personal data which are inaccurate in the light of the purposes for which they are processed are erased or rectified without delay ("correctness");
    e) kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the data are processed ("retention restriction");
    f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of appropriate technical or organisational measures ("integrity and confidentiality").

5. Data protection system.

The Entity's data protection system consists of the following elements:

1. Data Inventory. The ADO shall identify personal data resources in the Entity, classes of data, relationships between data resources, identification of uses of data (inventory) including:
   a) cases of processing of special categories of data and criminal data,
   b) cases of processing of data of persons whom the ADO does not identify
   c) data processing cases,
   d) profiling,
   e) data co-management.
2. Register. The ADO shall develop, maintain and keep a Register of Personal Data Processing Activities at the Entity (the Register). The Register is a tool for accounting for data protection compliance at the Entity.
3. Legal bases. The ADO shall ensure, identify, verify the legal basis for the processing of the data and record it in the Register including:
   a) maintains a system for managing data processing consents,
   b) inventories and details the justification for cases where the ADO processes data on the basis of the ADO's legitimate interest.
4. Handling of individual's rights. The ADO complies with its information obligations towards the individuals whose data it processes and ensures the handling of their rights by fulfilling the requests received in this respect, including:
   a) information obligations. The ADO shall provide persons with the information required by law at the time of data collection and otherwise, and shall organise and ensure that these obligations are documented;
   b) ability to execute requests. The ADO shall verify and ensure the ability of itself and its processors to effectively carry out each type of request.
   c) handling of requests. The ADO shall ensure that adequate inputs and procedures are in place to ensure that requests from individuals are dealt with within the timescales and in the manner required by the RODO and documented.
   d) breach notification. The ADO has procedures in place to determine the need to notify those affected by an identified data breach.
5. Minimisation. The ADO has policies and methods to manage minimisation (privacy by default), including:
   a) data adequacy management principles,
   b) the principles of data rationing and access management,
   c) rules for the management of the retention period and the verification of continued relevance.
   6. Security. The ADO shall ensure an adequate level of data security, including:
   a) carry out a risk analysis for a processing activity or category of data,
   b) carries out data protection impact assessments where the risk of interference with the rights and freedoms of individuals is high,
   c) adapts data protection measures to the risks identified,
   d) has an information security management system,

e) has procedures in place to identify, assess and report an identified data breach to the Data Protection Authority - manages incidents.

7. Processors. The ADO has rules for the selection of data processors for the Administrator, requirements for the terms of processing (entrustment agreements), rules for the verification of the execution of entrustment agreements.
8. Data export. The ADO has policies in place to verify whether the Subject transfers data to third countries (i.e. outside the EU, Norway, Liechtenstein, Iceland) or to international organisations, and to ensure the lawful conditions of such transfers, if any.
9. Privacy by design. The ADO manages changes affecting privacy. To this end, the procedures for launching new projects, investments in the Entity take into account the need to assess the impact of the change on data protection, risk analysis, ensuring privacy (and including the compatibility of processing purposes, data security and minimisation) already in the design phase of the change, investment or at the beginning of a new project.

6.Obligations of the Personal Data Controller

1. The ADO performs data protection tasks aimed at ensuring compliance with the provisions of the Regulation, including in particular:
   a) Oversees the development and updating of data protection documentation, including Policies and Instructions.
   b) Oversees compliance with the principles set out in the data protection documentation, including the Policy and the Manual.
   c) Ensures that the technical and organisational measures ensuring the protection of personal data at the Entity are adequate to the risks and categories of data processed.
   d) He shall ensure that the persons who are to be granted authorisations to process data are familiarised with the data protection regulations and rules adopted by the Entity by organising trainings for them, conducted by a person having appropriate knowledge and competence. The ADO may conduct the training personally. The data protection training card is attached as Appendix No. 1 to the Policy.
   e) Takes all necessary measures to properly safeguard personal data, including against:
   a) unauthorised access,
   b) unauthorised taking,
   c) uncontrolled change, loss,
   d) damage or destruction.
   f) Ensures the lawfulness of the processing of personal data in the Entity, and in particular ensures that:
      - on the basis of one of the legal grounds referred to in Article 6 or 9 of the Regulation,
      - in accordance with current legislation and good practice,
      - in accordance with the principles of expediency, factual correctness, relevance and time constraint.
   g) Authorises the processing of personal data of members of the Subject's staff to an individually defined extent.
   h) Supervises and ensures the lawful transfer of personal data (sharing and delegation).
   i) Provides users with appropriate workstations, including IT equipment, to enable the safe and lawful processing of personal data.
   j) Takes appropriate action in the event of a breach or suspected breach of the principles of secure processing of personal data.
   k) Carry out regular internal verification of compliance with data protection legislation, including checking.
   l) Ensures the correct operation of the IT system, in accordance with the purposes of processing personal data.
   m) Assigns each user an ID and password to the IT system and makes any modifications to the rights and deletes user accounts in accordance with the rules set out in the Manual.
   n) De-registers users.
   o) Manages the IT system in which personal data are processed, using an administrative password to access all workstations and servers from the position of administrator.
   p) Performs and supervises the repair, maintenance and decommissioning of computer equipment on which personal data is processed.

q) Performs and supervises the making of backups, their storage and periodic checking for their continued suitability for data restoration in the event of an IT system failure.
r) Trains users on procedures and instructions to ensure the protection of personal data and verifies the correct application of these procedures and instructions.
s) Explains all reported irregularities and incidents concerning data processing using IT means.

2. The ADO guarantees respect for the rights of data subjects, in particular the right to be informed about:
   a) data controller,
   b) the purpose, scope, manner and legal basis of the processing,
   c) the date by which and what data are processed,
   d) the source from which the data came,
   e) the manner in which the data are made available and the recipients of the data.
   f) the period for which the personal data will be kept and, where this is not possible, the criteria for determining that period;
   g) The right to request from the Controller access to, rectification, erasure or restriction of processing of personal data concerning the data subject, or the right to object to processing, as well as the right to data portability;
   h) if the processing is based on Article 6(1)(a) or Article 9(2)(a) RODO, information on the right to withdraw consent at any time without affecting the lawfulness of the processing carried out on the basis of consent before its withdrawal;
   i) the right to lodge a complaint with a supervisory authority;
   j) whether the provision of personal data is a statutory or contractual requirement or a condition for entering into a contract and whether the data subject is obliged to provide such data and what are the possible consequences of failing to do so;
   k) automated decision-making, including profiling, and, at least in these cases, relevant information about the modalities of such decision-making, as well as the significance and the envisaged consequences of such processing for the data subject.
3. The ADO guarantees that the rights of data subjects are respected with regard to:
   a) to request completion, updating, rectification, erasure, transfer of data, restriction of processing
   b) to make a reasoned request for the cessation of data processing,
   c) withdraw consent to the processing of personal data.
4. The ADO guarantees that the information obligation referred to in Article 13 of the Regulation will be complied with vis-à-vis the data subject.

7. Principles for granting authorisations to process data

1. Only persons trained in data processing and data protection in accordance with the Policy and the Manual, to whom the ADO has granted a written authorisation to process personal data, the specimen of which is attached as Appendix No. 2 to the Policy, may be allowed to process data at the Entity.
2. Each ADO employee authorized to process personal data, after receiving authorization to process personal data and after training, shall submit in writing a confidentiality declaration, the content of which shall be shaped depending on the scope of duties of a given employee and the template of which is attached as Appendix 3a and Appendix 3b to the Policy.
3. In case a person employed in the Entity on the basis of civil law forms of employment is allowed to process personal data, a confidentiality agreement shall be concluded with such person, after the ADO grants him/her in writing an appropriate authorization to process personal data.
4. The authorisation referred to in point 1. must be kept up to date. In the event of prolonged absence of the authorised person or cessation of some or all of his/her duties justifying the need to authorise him/her to process personal data, the authorisation must be cancelled.
5. The loss of authority to process personal data resulting from an authorisation to process personal data may occur due to:
6. termination of the employment or other legal relationship between the authorised person and ADO,
7. a change of job position at the ADO where it is not necessary to have access to the personal data files and the new job description does not show job duties related to the processing of personal data,
8. intentional breach of the data protection principles set out in the Regulation, the Policy and the Manual.
9. In case of loss of authorization to process personal data, the ADO shall immediately cancel the authorization to process personal data and make changes in the register of persons authorized to process data in the relevant data filing system.
10. The records of authorisations maintained by the ADO are set out in Appendix 4 to the Policy.

8. Legal basis of data processing

1. The processing of ordinary personal data is possible if one of the prerequisites set out in Article 6 of the Regulation is met, i.e. only if:
    a) the data subject has consented to the processing of their personal data for one or more specified purposes;
    b) the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
    c) processing is necessary for compliance with a legal obligation incumbent on the controller;
    d) the processing is necessary to protect the vital interests of the data subject or of another natural person;
    e) 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 controller;
    f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by 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, in particular where the data subject is a child.
2. The processing of special categories of data is possible if one of the prerequisites of Article 9 of the Regulation is met, i.e. only if:
    a) the data subject has given his or her explicit consent to the processing of that personal data for one or more specific purposes;
    b) the processing is necessary for the fulfilment of obligations and the exercise of specific rights by the controller or the data subject in the fields of labour law, social security and social protection;
    c) the processing is necessary to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving consent;
    d) the processing is carried out in the context of legitimate activities carried out with appropriate safeguards by a foundation, association or other non-profit-making body with a political, philosophical, religious or trade-union aim, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
    e) the processing concerns personal data manifestly made public by the data subject;
    f) the processing is necessary for the establishment, investigation or defence of claims or in the exercise of justice by the courts;
    g) the processing is necessary for reasons of substantial public interest, on the basis of Union law or Member State law, which are proportionate to the aim pursued, do not undermine the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational health care, assessment of a worker's fitness for work, medical diagnosis, the provision of health care or social security, treatment or the management of health care or social security systems and services on the basis of Union or Member State law or pursuant to a contract with a healthcare professional;

i) processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law;

j) processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes based on Union or Member State law.

3. The ADO shall document in the Register the legal basis of data processing for specific processing activities.
4. The ADO implements consent management methods to record and verify that a person has consented to the processing of their specific data for a specific purpose, consent to remote communications, and to record refusals of consent, withdrawal of consent and similar actions.

9. Collection and processing of personal data

Obtaining personal data

1. The personal data processed at the Entity are obtained directly from the data subjects or from other sources, within the limits permitted by law.

Use of personal data

1. The personal data collected shall only be used for the purposes for which they were, are or will be collected and processed. The controller shall only retain personal data in a form which permits the identification of the data subject for the time necessary to fulfil the purpose for which they are processed, in accordance with national legislation.
2. If it is necessary to provide access to documents and data which include personal data not directly relevant to the purpose of the access, it is imperative to anonymise such personal data.

Handling of individual rights and information obligations

1. The ADO takes care of the legibility and style of the information provided and communication with the persons whose data it processes.
2. ADO facilitates the exercise of persons' rights through various actions, including: posting on the website information or references (links) to information on persons' rights, how to exercise them at the Entity, including identification requirements, methods of contacting ADO for this purpose, possible price list for additional requests.
3. ADO ensures that legal deadlines for the fulfilment of obligations towards persons are met.
4. The ADO shall put in place adequate methods of identifying and authenticating persons for the purposes of exercising an individual's rights and information obligations.
5. In order to realise the rights of the individual, the ADO shall provide procedures and mechanisms to identify the data of specific individuals processed by the ADO, integrate that data, amend it and delete it in an integrated manner.
6. ADO documents the handling of information obligations, notifications and requests from persons.

Information obligation

1. Whenever data is collected directly from a data subject, the Data Controller shall inform the data subject in accordance with Appendix 9 of the Policy.
2. Whenever data is collected from sources other than the data subject, the Data Controller shall inform the data subject without delay, but no later than at the first contact with the data subject, in accordance with Appendix 10 to the Policy.
3. Whenever consent is taken from a data subject, consent clauses shall be used in accordance with Appendix 11 of the Policy.
   The ADO shall inform the person of a planned change in the purpose of processing.
   The ADO shall inform the person before lifting a restriction on processing.
   The ADO shall inform recipients of rectification, erasure or restriction of processing (unless this would require disproportionate effort or would be impossible).
4. The ADO shall inform the person about the right to object to the processing at the latest at the first contact with the person.
   The ADO shall notify the person of a personal data breach without undue delay if it is likely to result in a high risk of infringement of the person's rights or freedoms.

10. People's demands.

A record of the implementation of the data subject's requests is attached as Appendix 19 to the Policy.

1. Right of access to data
   Upon a person's request for access to his or her data, the Controller shall inform the data subject whether he or she is processing his or her data and shall inform the person of the details of the processing, in accordance with Article 15 of the RODO (the scope corresponds to the information obligation when collecting the data), and shall grant the person access to the data concerning him or her. Access to the data may be exercised by issuing a copy of the data, provided that a copy of the data issued in exercise of the right of access shall not be considered by the Subject as the first free copy of the data for the purpose of charging for copies of the data for the purpose of charging for copies of the data.
2. Data copies
   Upon request, the Entity shall issue to a person a copy of the data relating to that person and shall record the fact that the first copy of the data was issued. The Entity shall introduce and maintain a data copy price list, according to which it shall charge for subsequent data copies. The price of data copies shall be calculated on the basis of the estimated unit cost of handling a request for data copies.
3. Correction of data

   The entity shall rectify inaccurate data at the request of the person. The Subject shall have the right to refuse to rectify the data unless the person reasonably demonstrates the inaccuracy of the data for which rectification is requested. In the event of rectification, the Subject shall inform the person of the recipients of the data, upon the person's request.
4. Data completion

   The Subject completes and updates the data at the request of the person. The Subject has the right to refuse to complete the data if completion would be incompatible with the purposes of the data processing (e.g. the Subject does not need to process data that is unnecessary to the Subject). The Subject may rely on a statement by a person to supplement the data, unless it is insufficient in light of the Subject's established procedures (e.g. for obtaining such data), the law, or there are grounds to consider the statement unreliable.
5. Deletion of data
   At the request of the person, the Subject shall delete the data when:
   a) personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
   b) the person has withdrawn the consent on which the processing is based and there is no other legal basis for the processing;
   c) the person has lodged an effective objection to the processing of that data;
   d) personal data were processed unlawfully;
   e) personal data must be deleted in order to comply with a legal obligation provided for by law;
   f) the request shall relate to the child's data collected pursuant to consent for the purpose of providing information society services offered directly to the child. The entity shall determine how to handle the right to erasure in such a way as to ensure

that the right is exercised effectively while respecting all data protection principles, including security, and verifying that the exceptions referred to in Article 17(3) of the RODO do not apply.

If the data to be erased has been made public by the Subject, the Subject shall take reasonable steps, including technical measures, to inform other controllers processing the personal data of the need to erase and access the data. In the event of erasure, the Subject shall inform the person of the recipients of the data, upon the person's request.

6. Limitation of processing

The Entity shall carry out a restriction of data processing at the request of a person when:

a) the person questions the accuracy of the personal data - for a period allowing the Administrator to verify the accuracy of the data;
b) the processing is unlawful and the person, objects to the erasure of the personal data, requesting instead the restriction of its use;
c) The entity no longer needs the personal data, but it is needed by the data subject to establish, assert or defend a claim;
d) the person has objected to the processing on grounds relating to his or her particular situation - until it is determined whether the legitimate grounds on the part of the Controller override the grounds of the data subject's objection.

During the restriction of processing, the Controller shall keep the data, but shall not process them (not use them, not transfer them), without the person's consent, except for the purpose of establishing, asserting or defending claims, or for the purpose of protecting the rights of another natural or legal person on compelling grounds of public interest.

The Controller shall inform the person before lifting the restriction of processing.

In the event of restriction of processing, the Controller shall inform the person of the recipients of the data, at the person's request.

7. Data transfer

At the request of a person, the Controller shall issue in a structured, commonly used machine-readable format or transfer to another entity, if possible, the personal data concerning him/her which he/she has provided to the ADO, processed on the basis of that person's consent or for the purpose of entering into or performing a contract with him/her on the Entity's information systems. The request for data transfer is attached as Annex 20 to the Policy.

8. Objection in a specific situation

If a person raises an objection, motivated by his/her particular situation, to the processing of his/her data and the data are processed by the Controller on the basis of a legitimate interest of the Controller or on the basis of a task of public interest entrusted to the Controller, the Controller shall take the objection into account unless there are compelling legitimate grounds on the part of the Controller for the processing overriding the interests, rights and freedoms of the objector or grounds for the establishment, exercise or defence of claims.

9. Objection for scientific, historical research or statistical purposes

If the Entity carries out scientific or historical research or processes data for statistical purposes, a person may raise an objection, motivated by his or her particular situation, to such

processing. The Controller will respect such objection unless the processing is necessary for the performance of a task carried out in the public interest.

10. Objection to direct marketing
    If a person objects to the processing of their data by the Controller for the purposes of direct marketing (including possibly profiling), the ADO will respect the objection and cease such processing.
11. Transparent information and clear communication and modalities for the exercise of rights by the data subject
    The controller shall take appropriate measures to provide the data subject with all the information referred to in Articles 13 and 14 of the RODO in a concise, transparent, intelligible and easily accessible form in clear and plain language, in particular when the information is addressed to a child, and to carry out any communication with him/her about the processing. The information shall be provided in writing or by other means, including electronically where appropriate. If the data subject so requests, the information may be provided orally, provided that the identity of the data subject is confirmed by other means.
    The controller shall facilitate the exercise of the data subject's rights under the RODO.
    The controller shall, without undue delay - and in any case within one month of receipt of the request - provide the data subject with information on the action taken in relation to the request pursuant to points. 1-11 above. Where necessary, this time limit may be extended by a further two months due to the complexity of the request or the number of requests. Within one month of receipt of the request, the Controller shall inform the data subject of such extension, stating the reasons for the delay. If the data subject has communicated his/her request electronically, the information shall also be communicated electronically as far as possible, unless the data subject requests otherwise.
    If the Controller does not act upon the data subject's request, the Controller shall promptly - at the latest within one month of receipt of the request - inform the data subject of the reasons for not acting and of the possibility of lodging a complaint to the supervisory authority and of seeking judicial remedies.
    The information provided to the data subject and the communications and actions taken pursuant to points. 1-11 above shall be free of charge. If the requests made by the data subject are manifestly unreasonable or excessive, in particular because of their continuing nature, the controller may:
    a) charge a reasonable fee taking into account the administrative costs of providing the information, carrying out the communication or taking the action requested; alb
    b) refuse to act on the request.
    The onus is on the controller to demonstrate that the request is manifestly unreasonable or excessive in nature.

    If the Controller has reasonable doubt as to the identity of the natural person making the request referred to in Articles 15 to 21 of the RODO, the Controller may request additional information necessary to confirm the identity of the data subject.
12. Consent to processing of personal data
    Material relating to the non-statutory activities of the Entity may only be sent to those persons who have given their prior written consent to the processing of their personal data for this

purpose.
Candidates for employment with the Entity in the recruitment process are required to sign a written consent to the processing of their personal data.
Documents submitted for recruitment purposes are kept in the organisational unit that processes the data and are included in the employee's personal file.

11. Register of Data Processing Activities

1. The RCPD is a form of documentation of processing activities, acts as a data processing map and is one of the key elements enabling the fundamental principle on which the entire personal data protection system is based, i.e. the principle of accountability.
2. The ADO maintains a Register in which it inventories and monitors how it uses personal data.
3. The register is one of the basic tools enabling the Controller to account for most data protection obligations.
4. In the Register, for each data processing operation that the ADO has deemed separate for the purposes of the Register, he shall record at least: the name of the operation, the purpose of the processing, the description of the categories of persons, the legal basis of the processing with the specification of the categories of the Subject's legitimate interest if it is the basis of the processing, the method of data collection, the description of the categories of recipients, the information on the transfer after the EU/EEA, the general description of the technical and organisational measures of data protection.
5. The register of personal data processing activities is an element of the data protection documentation.
6. The register is attached as Appendix 12 to the Policy.
7. The Controller shall appoint a Data Protection Officer in the cases indicated in Article 37 of the RODO, or, in the absence of an appointment, shall explain this fact. The relevant documentation can be found in Annex 13.

12. Minimisation

1. The entity takes care to minimise data processing in terms of:
    a) the relevance of the data to the purposes (amount of data and extent of processing)
    b) access to data,
    c) storage time.

    Minimising the scope
2. The subject has reviewed the scope of data captured, the extent of processing and the amount of data processed for adequacy to the purposes of processing under the RODO.
3. The subject shall periodically review the amount of data processed and the extent of the processing at least once a year.
4. The entity carries out verification of changes as to the amount and extent of data processing as part of its change management procedures (privacy by design).

    Minimising access
5. The entity applies restrictions on access to personal data: legal (confidentiality obligations, authorisation ranges), physical (access zones, locking of premises) and logical (restrictions on authorisations to personal data processing systems and network resources where personal data reside).
6. The entity applies physical access control.
7. The entity shall update access rights when there are changes in the composition of staff and changes in the roles of persons and changes in processors.
8. The entity shall periodically review the established users of the systems and update them at least once a year.

    Minimisation of time
9. The Entity shall implement mechanisms to control the life cycle of personal data in the Entity, including verification of the continued relevance of the data against the deadlines and checkpoints indicated in the Register.
10. Data whose usefulness diminishes with the passage of time shall be deleted from the Subject's systems, as well as from the cache and master files. Such data may be archived and backed up on systems and information processed by the Entity. Procedures for the archiving and use of archives, the creation and use of backups shall take into account the requirements of data lifecycle control, including data deletion requirements.

13. Data sharing

1. The sharing of personal data is only possible if one of the aforementioned prerequisites for the processing of personal data is fulfilled.
2. The release of personal data may only take place following the submission of a request, a model of which is attached as Appendix 5 to the Policy, for the transfer or release of information.
3. The ADO shall keep a register of the sharing of personal data in order to ensure control of the sharing process. The model of the register is attached as Appendix No. 6 to the Policy.
4. The request for access to personal data should contain information making it possible to search for the requested personal data in the filing system and indicate their scope and purpose.
5. When sharing personal data, it must be stated that it can only be used for the purpose for which it was provided.
6. Where information on personal data being processed is requested following a written request from the data subject, the request shall be responded to within 30 days of receipt.
7. Access to personal data shall be refused if it would result in substantial damage to the personal rights of the data subject or of other persons and if the personal data are not substantially related to the motives of the applicant as indicated in the request.

14. Entrusting the processing of personal data

1. The ADO may entrust the processing of personal data to another third party by means of a written agreement, including in electronic form, a model of which is attached as Appendix 7 to the Policy.
2. A detailed list of personal data sets and entities entrusted with the processing of personal data can be found in Appendix 8 of the Policy.
3. The transfer of collections to an external entity for processing does not change the relevant ADO.
4. If the processing is to be carried out on behalf of the ADO, the ADO shall only use the services of such processors who provide sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the RODO and protects the rights of data subjects.
5. A processor may not use the services of another processor without the prior specific or general written consent of the Controller. In the case of general written consent, the Processor shall inform the Administrator of any intended changes concerning the addition or replacement of other processors, thereby giving the Administrator the opportunity to object to such changes.
6. The external entity entrusted with the processing of personal data is obliged to use the data entrusted to it only for the purposes and within the scope indicated in the contract concluded with it, as well as to maintain the confidentiality of the personal data entrusted to it for processing.
7. The external entity entrusted with the processing of data shall be obliged, inter alia, to:
    a) apply technical and organisational measures to ensure the protection of the processing of personal data appropriate to the risks and the category of data protected and, in particular, should secure the data against their access to unauthorised persons, against their taking by an unauthorised person, against their processing in violation of the Act, and against their alteration, loss, damage or destruction,
    b) the development and implementation of documentation on the processing and protection of personal data,
    c) ensure that only persons with an authorisation granted by the ADO are allowed to process the data,
    d) keeping records of persons authorised to process data,
    e) the obligation of persons who have been authorised to process personal data to maintain the confidentiality of such data and the ways and means by which they are secured.
    f) ensure control over what personal data has been entered into the file, when and by whom, and to whom it is transferred,
    g) inform ADO of the situation of subcontracting and indicate in the agreement the name of the entity, together with its contact details, to which the personal data will be subcontracted.

15. Security

1. The Entity shall ensure a level of security appropriate to the risk of violation of the rights and freedoms of natural persons as a result of the Entity's processing of personal data.
   Risk analysis and adequacy of security measures

2. The entity shall carry out and document analyses of the adequacy of personal data security measures. To this end:
3. The entity ensures an adequate state of knowledge of information security, cyber security and business continuity - either internally or with the support of specialised entities.
4. The entity categorises data and processing activities according to the risks they present.
5. The Entity shall carry out analyses of the risk of violation of the rights or freedoms of natural persons for processing activities or categories of data. The Entity shall analyse possible situations and scenarios of personal data breach, taking into account the nature, scope, context and purposes of the processing, the risk of violation of the rights or freedoms of natural persons with different probability of occurrence and severity of the risk.
6. The Entity shall determine the organisational and technical security measures that are feasible and assess the cost of implementing them. In doing so, the Entity shall determine the suitability and use such measures and approaches as:
   a) pseudonymisation,
   b) encryption of personal data,
   c) other cyber security measures that make up the ability to continuously ensure the confidentiality, integrity, availability and resilience of the processing systems and services,
   d) business continuity and disaster prevention measures, i.e. the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident.

   Data protection impact assessments
7. The subject shall carry out an assessment of the effects of the intended processing operations on the protection of personal data where, according to the risk analysis, the risk of violation of the rights and freedoms of persons is high.
8. The Entity shall apply the impact assessment methodology adopted at the Entity.
   Safety measures
9. The entity shall apply the security measures established as part of the risk and adequacy analyses and data protection impact assessments.
10. Personal data security measures are part of the Entity's information security and cyber security assurance measures and are further described in the procedures adopted by the Entity for these areas.
    Reporting violations
11. The entity shall have procedures in place to identify, assess and report an identified data breach to the Data Protection Authority within 72 hours of the identification of the breach.

16. Technical and organisational measures necessary to ensure the confidentiality, integrity and accountability of the processed data

1. Organisational safeguards:
   a) a security policy has been developed and implemented,
   b) an information system management manual has been developed and implemented,
   c) only persons authorised by the ADO are allowed to process the data,
   d) records of persons authorised to process data are kept,

e) members of staff and other persons processing personal data have been made aware of the data protection legislation and of the security features of the IT system,
f) members of staff and other persons processing personal data were obliged to keep it confidential,
g) the processing of personal data is carried out under conditions which protect the data against unauthorised access,
h) the presence of unauthorised persons on the premises where personal data are processed shall be permissible only in the presence of a person employed to process the personal data and under conditions which ensure data security,
i) written data processing entrustment agreements shall be used for cooperation with subcontractors processing personal data,
j) regular reviews of the Policy and the Manual are carried out,
k) the transfer of personal data to third parties (sharing and delegation) is supervised and carried out in accordance with the legal provisions.

2. The physical protection safeguards for personal data are described in Appendix 14 of the Policy.
3. The hardware security features of the IT and telecommunications infrastructure are applied to the physical components of the system, their connections and the operating systems. A detailed description of the security features is included in the Manual.
4. Safeguards for software tools and databases (technical and programmatic) apply to procedures, applications, programs and other software tools that process personal data. A detailed description of the safeguards is included in the Manual.

17. Risk analysis procedure and risk treatment plan

1. A risk analysis for the resources involved in the processes is carried out by the Data Controller using Appendix 15 of the Policy.
2. A risk analysis is carried out at least once a year and forms the basis for updating the way risks are handled.
3. Based on the results of the risk analysis carried out, the Data Controller implements ways to deal with the risks.
4. Each time, the Data Controller chooses how to deal with the risks and determines which risks and in what order they will be dealt with first.

18. Data export

1. The entity registers data exports, i.e. data transfers outside the European Economic Area (EEA in 2017 = European Union, Iceland, Liechtenstein and Norway), in the Registry.
2. In order to avoid situations of unauthorised data export, in particular in connection with the use of publicly available cloud services (shadow IT), the Entity periodically verifies users' behaviour and, where possible, provides equivalent solutions that comply with data protection law.

19. Privacy Design

1. The entity shall manage the privacy-impacting change in such a way as to enable adequate security of personal data and minimisation of processing.
2. To this end, the Entity's Project and Investment Principles refer to the principles of personal data security and minimisation, requiring a privacy and data protection impact assessment, consideration and design of the security and minimisation of data processing from the beginning of the project or investment.

20. DPIA (Data Protection Impact Assessment) procedure

1. The ADO shall carry out a data protection impact assessment of the intended processing operations where, according to the risk analysis, the risk of violation of rights and freedoms is high.
2. A DPIA is carried out whenever there is a significant change in the processing of personal data, e.g. a change of service provider, a change in the way data is processed, an exchange of resources involved in the process.
3. A DPIA shall be carried out together with a risk analysis at least once a year for processes which, as a result of a previous DPIA, showed a high risk to the rights and freedoms of data subjects.
   Safety measures
4. The ADO shall apply the security measures established as part of the risk analysis and adequacy of security measures and data protection impact assessments.
5. Data security measures are part of the Entity's information security and cyber assurance measures.

21. Procedure for dealing with security breaches of personal data

1. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorised disclosure of or unauthorised access to personal data transmitted, stored or otherwise processed, and in particular:
   a) unauthorised access to data,
   b) loss of media,
   c) unauthorised modification or destruction of data,
   d) sharing of data with unauthorised parties,
   e) illegal disclosure of data,
   f) obtaining data from illegal sources.
2. In the event of a breach in the security of the IT system or the occurrence of situations that may indicate a breach in the security of personal data, each member of staff is obliged to interrupt the processing of personal data and immediately notify the ADO or the immediate supervisor and then comply with the decisions taken by them.
3. A data breach notification should include:
   a) description of the symptoms of a personal data breach,
   b) identify the situation and the time at which the personal data breach was identified,
   c) identifying any relevant information that may indicate the cause of the breach,
   d) Identify the means of securing the system known to the person and any steps taken after the incident was disclosed.
4. Typical personal data security risks include:
   a) inadequate physical security of premises, equipment and documents,
   b) inadequate protection of IT hardware or software against leakage, theft and loss of personal data,
   c) non-compliance with data protection rules by staff.
5. Typical personal data security incidents include:
   a) external random events (fire in the facility/room, flooding, loss of power, loss of communications),
   b) internal random events (failures of the server, computers, hard disks, software, mistakes by IT specialists, users, loss / misplacement of data),
   c) deliberate incidents (intrusion into the IT system or premises, theft of data/equipment, leakage of information, disclosure of data to unauthorised persons, deliberate destruction of documents/data, viruses and other malware).
6. Where a threat or incident is identified, the ADO shall conduct an investigation to determine the cause of the threat or incident, what the potential consequences are and what action should be taken to rectify the condition.
7. The ADO also identifies those responsible for the breach and secures evidence in the case and documents its findings.
8. The ADO is also responsible for analysing security incidents or threats to the protection of personal data to determine whether there is a need for corrective or preventive action. If the ADO determines such a need, it shall identify the source of the incident or threat, the scope of the corrective or preventive action, the timeframe for implementation and the person responsible.

9. The ADO is responsible for overseeing the correctness and timeliness of the corrective or preventive actions implemented.
10. In the event of a personal data breach, the ADO shall, without undue delay - as far as possible, no later than 72 hours after the breach has been identified - notify it to the supervisory authority, unless the breach is unlikely to result in a risk to the rights or freedoms of individuals. A notification submitted to the supervisory authority after the expiry of 72 hours shall be accompanied by an explanation of the reasons for the delay.
11. The notification referred to in para. 10, must at least:
    a) describe the nature of the personal data breach, including, as far as possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records affected by the breach
    b) include the name and contact details of the Data Protection Officer or an indication of another contact point from which further information can be obtained;
    c) describe the possible consequences of a personal data breach;
    d) describe the measures taken or proposed by the Controller to address the personal data breach, including, where appropriate, measures to minimise its possible adverse effects.
12. If - and to the extent that - information cannot be provided at the same time, it may be provided successively and without undue delay.
13. All the above activities shall be recorded by the ADO. The ADO, once the emergency situation has been brought under control, shall prepare a final report outlining the causes and consequences of the event and conclusions, including staffing, to reduce the possibility of the event occurring in the future; a template for the final report is attached as Appendix 16 to the Policy.
14. The register of breaches is attached as Appendix 17 to the Policy.
15. If a personal data breach is likely to result in a high risk of infringement of the rights or freedoms of natural persons, the Controller shall, without undue delay, notify the data subject of such breach.
16. The notification referred to in paragraph 15 shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in 15.
17. The notification referred to in paragraph 15 shall not be required in the following cases:
    a) The controller has implemented appropriate technical and organisational security measures and these measures have been applied to the personal data affected by the breach, in particular measures such as encryption to prevent reading by persons not authorised to access such personal data;
    b) The controller has subsequently applied measures to eliminate the likelihood of a high risk of infringement of the rights or freedoms of the data subject referred to in point a);
    c) it would require a disproportionate effort. In such a case, a public notice shall be issued or a similar measure shall be taken by which the data subjects are informed in an equally effective manner.
18. If the controller has not yet notified the data subject of a personal data breach, the supervisory authority, taking into account the likelihood that the personal data breach will result in a high risk, may require the controller to do so or may determine that one of the conditions referred to in paragraph 17 has been met.
19. A flow chart for dealing with a data breach is attached as Appendix 21 to the Policy.

20. The checklist - how to deal with a data breach is attached as Appendix 22 to the Policy.

22. Policy reviews and system audits

1. The Policies should be reviewed/checked at least once a year to ensure that they are up to date and that the status declared in them is in accordance with the law. In case of significant changes concerning the processing of personal data, the ADO may order a review of the Policy as required.
2. The following are authorised to control the state of personal data protection in the Entity:
   a) ADO,
   b) persons designated by ADO.
3. The ADO shall analyse whether the Policy and other data protection documentation is adequate to:
   a) changes to the design of the IT system,
   b) organisational changes of the ADO, including changes in the status of persons authorised to process personal data,
   c) changes to existing law.
4. Once a year, all IT systems that process personal data and physical and personal security safeguards are audited.
5. The ADO shall prepare an audit plan taking into account the scope and physical, time and personnel needs.
6. The equipment, the ICT system, the implementation of security measures and compliance with the Policy are subject to control.
7. The ADO may, as appropriate, conduct an internal audit of the compliance of data processing with data protection legislation.
8. The scope, conduct and results of the audit shall be documented in writing in a protocol.
9. The ADO may commission an external audit by a specialised entity. A model report is attached as Annex 18 to the Policy.

23. Final provisions

1. This Policy is an internal document and must not be made available to unauthorised persons in any form.
2. The user is obliged to declare that he/she has been made aware of the provisions of the Ordinance and the instructions in force at ADO and that he/she undertakes to comply with them.
3. A statement confirming that the user has been made aware of the data protection legislation and instructions in force at ADO, and that he/she undertakes to comply with them, shall be kept in the employee's personal file.
4. All regulations relating to information systems set out in the Policy also apply to the processing of personal data in databases maintained in any other form.
5. All authorised persons are required to apply the provisions contained in this Policy when processing personal data.
6. Cases of unjustified failure to comply with the obligations arising from this document may be treated as grounds for prosecution of the person concerned in accordance with the legal relationship between him/her and ADO.
7. The provisions of the Ordinance and other acts, including regulations, shall apply to matters not covered by the Instruction.

List of annexes to the Policy

1. Annex 1 to the Policy - Data Protection Training Card
2. Attachment No. 2 to the Policy - Authorisation to process data
3. Annex 3a to the Policy - Declaration of Confidentiality - Staff
4. Appendix 3b to the Policy - Declaration of confidentiality - technical, cleaning staff
5. Annex 4 to the Policy - Register of authorisations
6. Annex No. 5 to the Policy - request for access to data
7. Annex 6 to the Policy - Register of disclosures
8. attachment no. 7 to the Policy - model agreement on entrustment of personal data processing
9. Annex 8 to the Policy - Register of entrustments
10. Annex 9 to the Policy - model information clause 1
11. Annex 10 to the Policy - model information clause 2
12. attachment no. 11 to the Policy - model consent clause for data processing
13. Annex No. 12 to the Policy - Register of processing operations
14. Annex No. 13 to the Policy - Checklist - Appointment of the Data Protection Officer
15. Annex 14 to the Policy - Rules for the protection of premises
16. Annex 15 to the Policy - Risk Analysis
17. Annex 16 to the Policy - model data breach report
18. Annex 17 to the Policy - Data Protection Breach Register
19. Annex No. 18 to the Policy-Report on the verification of the compliance of the processing of personal data with the provisions on their protection
20. Annex 19 to the policy-Record of fulfilment of data subject's requests
21. Annex 20 to the Policy - Request for data transfer
22. Annex No. 21 to the Policy - Data Protection Breach Handling Scheme
23. Annex 22 to the Policy - Checklist on how to deal with data protection breaches