DATAMANAGEMENT POLICY

EWG Rail Ltd.
Applicable: 30.08.2024.

Introduction

EWG Rail Private Limited Company (Cg.01-10-049688; tax number: 26242387-2-41. hereinafter referred to as the "Company" or the "Controller") is committed to protecting the personal data of its employees and business partners, as well as third parties who come into contact with it, including visitors to the website https://ewgrail.com/ (hereinafter referred to as "Data Subjects"), and attaches great importance to respecting the right of self-determination. This Privacy Policy and in particular the rules and procedures contained herein are designed to ensure that the Data Controller complies with the applicable international and national legal provisions on data protection, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "GDPR") and Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter "Info tv."). The Data Controller shall act in accordance with the provisions of this Privacy Policy (hereinafter referred to as the "Privacy Policy") and other internal rules and instructions. This Privacy Policy shall be reviewed annually and compliance with the applicable legal provisions shall be verified. Management is responsible for the content of this Privacy Policy, compliance with it and the proper design of its processes.

Who has to comply with this policy?

Employees of the Company, persons employed by the Company in other employment relationships and data processors engaged by the Company must comply with this Policy and must perform their work in accordance with the provisions of this Policy.

MAIN RELEVANT LEGISLATION

The Data Controller shall act in accordance with the following legal requirements in its processing, as set out in this Policy:

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 Regulation (EC) No 95/46/EC (General Data Protection Regulation) (hereinafter "**GDPR**")

Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: **Info tv.**)

Act V of 2013 on the Civil Code (hereinafter: **Civil Code**)

Act C of 2012 on the Criminal Code (hereinafter: Criminal Code)

Act I of 2012 on the Labour Code (hereinafter referred to as "**Act** I of 2012 on the Labour Code")

Act XLI of 2012 on Passenger Transport Services (hereinafter referred to as: **Passenger Transport Act**)

Act CLV of 1997 on Consumer Protection (**Fgy. tv.**)

Act C of 2000 on Accounting (hereinafter: **Accounting Act**)

Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: **Pmt.**)

Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation (hereinafter: the **Act**)

PURPOSE OF THE CODE

By applying and complying with the rules set out in this Privacy Policy, the Company can ensure the practical implementation of the provisions of the applicable legislation, in particular the GDPR, through internal instructions and procedures based on this Privacy Policy. In this context, the Company sets out, through this Privacy Policy, the framework within which

- ensures that the fundamental rights of Data Subjects to the protection of personal data are respected, and that data security requirements are complied with and enforced;
- regulates the process of planning, assessing and reviewing the risks to which its data are subject;
- regulates practices to prevent unauthorised access to data and sets out rules to prevent unlawful alteration, unauthorised use and unauthorised disclosure of data;
- determine the precise and secure arrangements for the processing, use, transfer and destruction of data by electronic means;
- sets out the procedures and minimum content required for the provision of information to data subjects and the exercise of their rights to information;
- sets out the rules to be followed in the event of a personal data breach and in the administrative procedure;
- sets out the minimum procedures to be followed in order to improve the organisation's data protection awareness.

Detailed internal instructions and procedures should be developed in accordance with this Privacy Policy, taking into account the actual processes and documented as necessary.

1. GENERAL PART

1.1. INTERPRETATIVE PROVISIONS

Introduce concepts when applying the rules:

"personal data" means 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, 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 - thus, any data by reference to which the data subject can be identified, such as name, address, telephone number, GPS data, IP address, etc.

"special categories of personal **data" means** any data that fall within special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

"processing" means any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction - that is, any operation or set of operations which is performed upon the data, such as recording, consultation, organisation, etc.

"transfer" means the making available of personal data to a specified third party.

"disclosure" means making personal data available to any person.

"erasure" means the rendering of personal data unrecognisable in such a way that it is no longer possible to recover it.

"pseudonymisation" means the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no natural person who is identified or identifiable can be linked to that personal data;

"filing system" means a set of personal data, structured in any way, whether centralised, decentralised or structured according to functional or geographical criteria, which is accessible on the basis of specified criteria

"data inventory": a document used to assess the scope and nature of the personal data processed by the controller.

"controller" means a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for the designation of the controller may also be determined by Union or Member State law; - the controller in this case is the Company;

"**data processor**" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; *a data processor is any person or undertaking which, on behalf of and under the instructions of the Company, carries out specific operations with personal data (payroll service provider, hosting service provider, software provider, occupational health professional, etc.)*

"**recipient**" means a natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party. Public authorities which may have access to personal data in the context of an individual inquiry in accordance with Union or Member State law are not recipients; the processing of such data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing; - *a recipient is any person, company or authority to whom the data are transferred or who has access to the data: e.g. tax authority, data processor, recruitment agency, etc.)*

"**third party**" means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data; - *any person or company which cannot normally be associated with the processing;*

"third country" means any country outside the European Economic Area.

"**data subject's consent**": a voluntary, specific, informed and unambiguous indication of the data subject's wishes, by which the data subject signifies his or her agreement to the processing of personal data concerning him or her by means of a statement or an unambiguous act of affirmation; - *this may be a written declaration of consent, ticking the consent checkbox on the website, etc., it is important to note that, from a data protection perspective, silence cannot constitute consent)*

"**personal data** breach" means 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; - *any event that compromises data, such as. hacker attack, archive burn down, but this includes for example loss of laptop, mobile phone, data media containing data, sending personal data to the wrong e-mail address, unsecure storage of personal data (e.g. payment slips thrown in the trash); unsecure transmission of data, unauthorised copying of customer and customer partner lists, etc.)*

"Breach of Privacy Incident" means an incident that results in the unauthorized or accidental disclosure of, or access to, personal data.

"Integrity incident" means an incident that results in the unauthorised or accidental alteration of personal data.

"availability incident" means an incident that results in the unauthorised or accidental loss or destruction of personal data.

"data security" means any technical or organisational measures designed to ensure the security of the personal data processed, whether physical, optical or organisational, in particular measures to protect against unauthorised or unlawful processing, accidental loss, destruction or damage to personal data.

1.2. PRINCIPLES OF DATA MANAGEMENT

Personal data

- processing must be lawful, fair and transparent for the data subject ("lawfulness, fairness and transparency"); - which means that data must be processed only in accordance with the relevant legal provisions and the data subject must be given the opportunity to be properly informed of the circumstances of the processing (purposes, legal basis, duration, etc.);
- collected only for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes (further processing for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes is allowed) ("purpose limitation"); - which means that data processed for a specified purpose may be used for other purposes only in exceptional cases;
- must be adequate and relevant for the purposes for which the data are processed and limited to what is necessary ("data minimisation"); - which means that personal data may only be processed if there is no other way to achieve the specified purpose;
- be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes of the processing are erased or rectified without undue delay ("accuracy"); - which means that changes to the data must be implemented as soon as possible;
- be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('limited storage'); this means that once the purpose has been achieved (maximum period of processing), the data must either be erased or rendered anonymous so that the data can no longer be used to identify the data subject;
- be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage ("integrity and confidentiality"), by using appropriate technical or organisational measures; - require appropriate IT and other security measures to prevent unauthorised access to the data;
- The controller is responsible for compliance with the above and must be able to demonstrate such compliance ("accountability") - the controller shall set out its data

management processes in internal instructions and policies so that the processes can be accurately followed in the organisation (and where necessary, verified to the authorities).

1.3. PURPOSES AND LEGAL GROUNDS FOR PROCESSING

Purposes of data processing

The purpose of the processing shall be determined by the Company for each processing operation separately before the processing starts.

In general, we process the Data Subjects' data for the purposes of the Company's business activities, contractual rights and obligations.

Legal basis for data processing

The legal basis for the processing is also determined by the Company for each individual processing.

The processing of personal data is lawful only if and insofar as at least one of the following conditions is met: a) The data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes:

The data subject's consent is always voluntary and can only be given through some active act (silence is not consent), such as written consent (either in a separate statement or, for example, by signing a contract where the contract itself contains consent), ticking a checkbox on an electronic interface, clicking on a "I agree" button, etc.).

Consent must/may be given separately for each processing operation.

The data subject has the right to withdraw his or her consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal, i.e. consent may only be withdrawn prospectively. Withdrawal of consent must be made as easy as giving it, i.e. it can be given in the form of a written letter or a statement by telephone or e-mail.

The consent of a person under 16 years of age or a person with reduced capacity to act is valid if given by the guardian/carer of the person having parental authority/limited capacity in the case of a person with parental authority/limited capacity. In case of doubt, the person concerned shall be presumed not to have given his or her consent.

The data subject's consent shall be considered a valid legal basis for processing where it is a freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject signifies, by a statement or by an act unambiguously expressing his or her consent, that he or she signifies his or her agreement to the processing of personal data concerning him or her.

The data subject's consent must ensure that the data subject has a real choice, and that there can be no doubt about the "informed" nature of the consent.

Consent is not considered voluntary if its consequences would undermine the individual's freedom of choice.

Furthermore, with the consent of the data subject:

- the controller must be able to demonstrate that the data subject has given his or her consent to the processing of his or her personal data;
- the controller must ensure that the data subject can withdraw consent at any time and must allow the withdrawal of consent in the same simple manner as the giving of consent;
- silence, ticking a box or inaction does not constitute consent;
- consent shall not be considered to be given voluntarily if the data subject does not have a real or free choice and is not in a position to refuse or withdraw consent without any prejudice;
- consent cannot be considered voluntary if it does not allow for separate consent for different personal data processing operations;
- consent cannot be considered voluntary if the performance of the contract (for example, the provision of a service) is made subject to consent to processing which is not necessary for the performance of the contract;
- consent shall not constitute a valid legal basis where there is a clear unequal relationship between the data subject and the controller;
- where the controller obtains the data subject's consent through a written statement, the request for consent must be clearly and unambiguously separated from the rest of the contract and must be drafted in clear and plain language by the controller.

Before obtaining consent, the Data Controller, a person employed by or otherwise engaged in an employment or service relationship with the Data Controller, or a processor acting on the basis of a contract with the Data Controller shall provide the data subject with appropriate information. The information may be provided by means of the information indicated in the consent form provided for that purpose. In that case, the data subject must be given sufficient time to acquaint himself with the information and to understand it.

The data subject shall have the right to request further information and clarification from the Data Controller, from a person employed by or otherwise engaged in an employment relationship with the Data Controller or from a data processor acting on the basis of a contract with the Data Controller. The provision of information or clarification is mandatory.

(b) The processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract (contractual obligation):

If the performance of the contract is not possible without the processing of personal data, this may be a legitimate ground for processing. In such cases, the data subject's specific consent is not required.

Data processing in the context of the performance of a contract most often relates to the personal data of the contracting parties as recorded in the contract (name, address, etc.), but may also include, for example, data relating to the use of a service. This is for example the case when a personalised invoice is issued to the customer during a purchase.

Personal data may be processed for the purpose of concluding a contract if:

- the contract is concluded by the Data Controller with the data subject;
- the data subject provides the data to the Data Controller;
- the data are necessary for the conclusion of a contract between the Data Controller and the data subject.

Personal data may be processed for the performance of the contract if:

- there is a contract to which the person concerned is a party;
- the contract is valid;
- the processing is actually necessary for the achievement of the general objective of the contract.

The necessity requirement is a precondition for the application of the contractual legal basis. This requirement cannot be reduced to an examination of contractual terms alone, but also presupposes consideration of data protection guarantees and the principles set out in the GDPR, in particular the principles of fairness, purpose limitation and data minimisation. Thus, if the processing is useful but not objectively necessary for the performance of the contract, the contractual legal basis does not apply.

c) processing is necessary for compliance with a legal obligation to which the Controller is subject (legal obligation)

The performance of a legal obligation may constitute a legal ground for processing personal data where:

- it is required by EU or national law;
- the provision contains an obligation directly applicable to the Data Controller;
- the provision serves a general interest objective;
- the provision is proportionate to the legitimate aim pursued.

The purpose of processing based on legislation is to fulfil obligations under that legislation. Legally mandated processing is considered as mandatory processing, the scope and duration of which are always determined by the applicable legislation. A large number of laws impose an obligation to process data. It is important to note that legal obligations are not optional and must therefore always be complied with. For example, data processing in relation to tax, payroll obligations, data processing in relation to mandatory aptitude tests, records taken in the management of warranty/guarantee claims, etc.) The relevant legal section should be indicated in each case.

d) Processing where the processing is necessary for the protection of the vital interests of the data subject or of another natural person

In a specific case where the data subject is not able to pursue his or her own interests or is prevented from doing so, it is possible to ensure that his or her data are processed only to the extent necessary and only for the duration of the prevention in the context of the pursuit of a vital interest.

(e) Processing where the 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 (public authority processing). The Company is not a public authority and does not process data on such legal basis.

(f) Processing where the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party (legitimate interest), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child

The legitimate interests of the Controller, including the controller with whom the personal data may be shared, or of a third party may constitute a legal ground for processing, provided that the interests, fundamental rights and freedoms of the data subject do not override the legitimate interests of the data subject, taking into account the reasonable expectations of the data subject in his or her relationship with the controller.

The legitimate interest of the Controller, including the controller with whom the personal data may be disclosed, or of a third party shall not constitute a legal basis for processing where the processing is carried out by the Controller, including the controller with whom the personal data may be disclosed, or by a third party in the context of the performance of a public task.

In order to establish the existence of a legitimate interest, it is necessary to consider, inter alia, whether the data subject could reasonably expect, at the time and in the context of the collection of the personal data, that processing for the purposes in question would take place.

The interests and fundamental rights of the data subject may override the interests of the Controller if the personal data are processed in circumstances in which the data subjects do not expect further processing.

The processing of legitimate interest as a legal basis requires the Data Controller to carry out the so-called interest balancing test. The balancing of interests test consists of the following steps:

- the legitimate, clear and present interest of the controller must be established;
- identify the fundamental rights and freedoms of the data subject and take into account the expectations of the data subject;
- analyse the necessity and proportionality of the processing;
- further measures should be identified to reduce the impact of data processing.

In all cases, the Company shall document the interest test in writing and the Data Subject may request information on any stopping of the interest test.
The Interest Assessment Test is described in detail in section 2.1.

1.4. DATA SUBJECTS' RIGHTS IN RELATION TO DATA PROCESSING

Prior information requirement

At the time of obtaining the personal data, the data subject must be informed of the fact, purpose, legal basis, scope of the data processed, the method, duration or criteria for determining the duration of the processing, the rules on data portability, the right to lodge a complaint with the supervisory authority.

In addition to the information referred to in the previous paragraph, the data subject shall be expressly informed of the possibility to exercise the right to object and the information shall be clearly displayed separately from any other information.

For information:

(a) be provided to applicants on the page where the vacancy notice is published, in accordance with the relevant data management notice;

b) to persons who establish an employment relationship or other employment relationship with the Data Controller, at the time of the establishment of the legal relationship, with the content of the relevant data management information;

The information referred to in point (a) shall be made available on the website of the Data Controller in a concise, transparent and easily accessible form, in clear and plain language.
The information referred to in point (b) shall be provided in electronic form at the time of the establishment of the legal relationship, and the person concerned shall provide written proof of this in the form of a paper declaration.

Right of access of the data subject

At the request of the data subject, the competent administrator responsible for the processing shall, within 30 days of receipt of the request, provide information on the ongoing processing of the data subject.

The data subject has the right to access personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom or which the personal data have been or will be disclosed, including in particular recipients in third countries or international organisations;

(d) where applicable, the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;

(e) the right of the data subject to obtain from the controller the rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of such personal data;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the data have not been collected from the data subject, any available information concerning their source.

Access to personal data must be ensured in such a way that the data subject is as far as possible prevented from becoming aware of the personal data of another person. An exception to this may be made for personal data which relate to both the data subject and another person.

The Data Controller may restrict or deny the data subject's right of access proportionate to the aim pursued, where such a measure is strictly necessary:

a) the effective and efficient conduct of investigations or proceedings involving the Data Controller, in particular criminal proceedings;

b) the effective and efficient prevention and detection of criminal offences;

c) the enforcement of penalties and measures against offenders;

d) the effective and efficient protection of public security;

(e) the effective and efficient defence of the external and internal security of the State, in particular national defence and national security; or

(f) to ensure the protection of the fundamental rights of third parties.

If the Data Controller denies or restricts the data subject's right of access as set out above, the Data Controller shall inform the data subject in writing without delay, stating the reasons for the measure, provided that the purpose of the restriction or denial is not jeopardised. In the notification, the Data Controller shall specifically draw the attention of the data subject to the fact that he or she may exercise the right of access with the assistance of the supervisory authority.

The Data Controller shall keep a record of its actions in relation to the exercise of the right of access in the register in Annex ... to the Rules. Where the Data Controller restricts or denies the Data Subject's right of access, it shall state the legal and factual reasons for the measure.

The right to rectification

The data subject shall have the right to obtain from the Data Controller, upon his or her request and without undue delay, the rectification of inaccurate personal data relating to him or her. Having regard to the purposes of the processing, the data subject shall have the right to obtain the rectification of incomplete personal data, including by means of a supplementary declaration.

At the request of the data subject, the competent administrator responsible for data processing shall correct inaccurate personal data relating to the data subject without undue delay. Taking into account

the purpose of the processing, the data subject shall also have the right to request the completion of incomplete personal data, including by means of a supplementary declaration.

Any recipient to whom or with whom the personal data have been disclosed must be informed of the modification, unless this proves impossible or involves a disproportionate effort. The data subject shall be informed of those recipients upon request.

Right to erasure ("right to be forgotten")

The data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her without undue delay at his or her request, and the controller shall be obliged to erase personal data relating to him or her without undue delay if one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed (the purpose of the processing has been fulfilled)
- the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- the legal basis for the processing is the legitimate interest of the controller and the data subject objects to the processing and there is no overriding legitimate ground for the processing or the data subject objects to processing for direct marketing purposes;
- the personal data have been unlawfully processed;
- the personal data must be erased to comply with a legal obligation under EU or Member State law applicable to the controller (e.g. if required by a public authority).

If the Controller has disclosed the personal data and is required to delete it as set out above, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the controllers that process the data that the data subject has requested the deletion of the links to or copies or replicas of the personal data in question.

The Data Controller is not obliged to delete the data if the processing is necessary

- to exercise the right to freedom of expression and information;
- for the purposes of complying with a legal obligation that requires the controller to process personal data;
- in certain cases, on grounds of public interest in the field of public health;
- for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, where deletion would be unlikely to achieve or would seriously undermine the achievement of that purpose;
- to bring, enforce or defend legal claims.

All recipients to whom or with whom the personal data have been disclosed must be informed of the erasure, unless this proves impossible or involves a disproportionate effort. The data subject shall be informed of those recipients upon request.

Right to restriction of processing

The data subject shall have the right to obtain, at his or her request, the restriction of processing by the controller if one of the following conditions is met:

- the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the controller to verify the accuracy of the personal data (*i.e. until it is certain that the data processed are accurate*);
- the data processing is unlawful, but the data subject opposes the erasure of the data and instead requests the restriction of their use (*because the data processing may subsequently become lawful and the data will not need to be recorded again*);
- the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing based on legitimate interest; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

If the processing is restricted as described above, such personal data, except for storage, may only be processed with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for important public interest. The data subject shall be informed in advance of the lifting of the restriction on processing.

Any recipient to whom or with which personal data have been disclosed must be informed of the restriction of processing, unless this proves impossible or involves a disproportionate effort. The data **subject** shall be informed of those recipients upon request.

The right to data portability

At the request of the data subject, the competent administrator responsible for the processing shall ensure the portability of personal data, provided that the following conditions are met:

a) the personal data have been provided to the Data Controller by the data subject;

(b) the legal basis for processing is consent or a contract between the data subject and the controller;

c) processing is carried out by automated means;

(d) the processing of personal data does not adversely affect the rights or freedoms of others.

In exercising the right to data portability, the Data Controller shall provide the personal data to the data subject in a structured, commonly used, machine-readable format (PDF/XML).

The data subject may request that the Controller transfers the personal data directly to another controller. The data subject may exercise this option only if it is technically feasible.

The Data Controller is also obliged to make personal data available on paper in order to facilitate the exercise of the right of access**.**

The right to protest

The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data in the public interest or based on the legitimate interests of the Company, including profiling based on the aforementioned provisions. In such a case, the controller may no longer process the personal data unless the controller demonstrates compelling

legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
Where personal data are processed for direct marketing purposes (e.g. marketing, newsletter, etc.), the data subject has the right to object at any time to the processing of personal data concerning him or her for such purposes, including profiling, if it is related to direct marketing.

If the data subject objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for those purposes.

Right to lodge a complaint with a supervisory authority
Without prejudice to any other administrative or judicial remedy, any data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes the provisions of the GDPR.
The supervisory authority shall investigate the subject matter of the complaint and inform the complainant within a reasonable time of the developments and results of the investigation, in particular if further investigation or cooperation with another supervisory authority becomes necessary. Following a complaint, the supervisory authority shall be entitled to initiate proceedings against the controller.

If the controller fails to act on the data subject's request, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the possibility for the data subject to lodge a complaint with a supervisory authority and to exercise his or her right of judicial remedy.

The exact contact details of the Hungarian supervisory authority are indicated in the Privacy Policy.

Restrictions
EU or Member State law applicable to the controller or processor may, in certain cases, limit the rights of data subjects as set out above by legislative measures.

2. PROCEDURAL INSTRUCTIONS

2.1. Balance of interests test

In all cases where the legal basis for the processing is the legitimate interest of the Company, a balancing of interests test must be carried out and the result must be properly documented. The form for the Interest Weighing Test is attached as Annex 1 to these Data Processing Instructions.

2.1.1 Steps of the Interest Weighing Test

1. **Step 3:** Determining the purpose of the processing

Personal data may only be processed for predefined, legitimate purposes. The so-called "stockpiling" processing, where data is collected for an unforeseen purpose, is prohibited. The purpose of the processing must be clearly and intelligibly stated.

2. **Step 3:** Clear definition of legitimate interest

The legitimate interests to be used as the legal basis for processing must be specified precisely and clearly, in sufficient detail to be compatible with the fundamental rights and freedoms of data subjects. The legitimate interest must be an interest pursued by the controller which is relevant to its current activities. Overly vague or theoretical interests are not appropriate.

That is, the legitimate interest

- be legal (i.e. comply with EU and/or national law);
- must be sufficiently clear (i.e. sufficiently precise) to allow the balancing of interests test to be carried out in relation to the interests and fundamental rights of the data subjects;
- must be a real and present interest (i.e. not a theoretical interest).

A legitimate interest is in particular:

- direct marketing, market research
- legal claims, including the recovery of claims through extra-judicial procedures
- preventing fraud, misuse of services or money laundering
- employee checks
- promoting physical, IT and network security

3. **Step 3:** Determining whether the processing is strictly necessary for the purposes of the interest pursued

This step should consider whether the purpose of the processing can be achieved without processing the data. If yes, then the processing is unnecessary and the processing cannot be carried out. If the purpose cannot be achieved without the processing, then the balancing of interests test can be continued.

4. **Step 3:** Assess whether the interests of the controller override the fundamental rights or interests of the data subjects

To determine this, the following circumstances should be taken into account:

- the nature of the controller's interest (fundamental right, public interest, statutory right, commercial interest);

- any harm suffered by the controller, third parties or the wider community in the event of failure of processing;
- the nature of the data (confidential or sensitive in a broad sense);
- the legal situation of the data subjects (minor, employee, etc.) and the controller (e.g. whether the company is in a dominant market position);
- the way the data is processed (profiling, affecting a wide range of people);
- the fundamental rights and/or interests of data subjects which may be affected;
- the reasonable expectations of stakeholders;
- the effects on data subjects compared with the benefits of the controller's processing.

Generally speaking: evaluating whose interests are more important and why.

5. **Step 3:** Drawing up the final balance sheet taking into account the additional guarantees

Identify measures to reduce the potential impact of data processing:

- data minimisation (only the data that is strictly necessary should be processed and data should be deleted immediately after the purpose has been achieved, the deletion function should be automated if possible)
- implementing technical and organisational measures to ensure that data cannot be used to make decisions about individuals or for other actions (functional separation)
- extensive use of anonymisation techniques, data aggregation, privacy-enhancing technologies;
- the right to object (opt-out).

6. **Step 3:** Ensuring transparency - documenting the decision

- The process of the balancing of interests test, the circumstances considered at each step, must be documented in sufficient detail to demonstrate that the decision is well founded
- In case of doubt, the involvement of a data protection officer/expert is required
- Where the processing activity poses a high risk to the rights and freedoms of data subjects, a data protection impact assessment should also be carried out

2.1.2 Results of the Interest Weighing Test

The Interest Assessment Test must be carried out for all data processing activities of the Company where the Company's legitimate interest is the legal basis for the processing. The balancing exercise should cover all the specificities of the Company's operations.

All Interest Assessment Tests must be documented in writing.

The information notice on data management should provide simple, clear and transparent information to data subjects on the results of the Interest Assessment Test.

2.1.3 Review of the Interest Screening Test

The findings of the Interest-Balancing Test should be reviewed at least once a year, and in any case whenever there is a change in the circumstances of data management.

In addition, where a data subject objects to processing, the balancing of interests test should be reviewed for the individual data subject, taking into account his or her own individual circumstances, and the findings of the review of the balancing of interests test should be communicated to the data subject when the objection is considered.

2.2. RISK ASSESSMENT AND DATA PROTECTION IMPACT ASSESSMENT

The data protection risk assessment and the data protection impact assessment provide a solution on how to identify the potential risks for each processing operation and, where required, how to complete the data protection impact assessment and how to manage the risks.

The national data protection authority has issued a position paper on which activities are subject to a mandatory data protection impact assessment. The current list is available on the NCA website and should be checked when planning each processing operation.

Risk assessment and evaluation, as with all similar processes, requires a common sense approach and a full understanding of the overall objectives, which are to protect personal data to the fullest extent possible and to comply with the requirements of the GDPR.

According to the GDPR, failure to comply with the requirements of the Data Protection Impact Assessment will result in a fine by the supervisory authority. Failure to carry out a Data Protection Impact Assessment where it would be mandatory (Article 35(1) and (3-4)), failure to properly implement a Data Protection Impact Assessment (Article 35(2) and (7), (9)) and failure to consult the supervisory authority in advance can result in an administrative fine of up to €10M, or for undertakings up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The risk assessment procedure diagram is attached as Annex 2 to these Privacy Instructions.

2.2.1 Determination of necessity and circumstances

In line with the risk-based approach set out in the GDPR, an impact assessment is not mandatory for each individual processing operation. An impact assessment is only required where the processing of personal data is likely to present a "high" risk to the rights and freedoms of natural persons (Article 35(1) GDPR). The mere fact that the conditions for the obligation to carry out an impact assessment are not met does not in itself diminish the general obligation to take the necessary measures to identify and adequately address the risks to the rights and freedoms of data subjects, which is the risk assessment. In practice, this means that risks arising from processing activities involving personal data must be assessed on an ongoing basis.

The data protection impact assessment/risk assessment must be carried out prior to the processing and is a decision-making tool for the processing.

The data protection impact assessment/risk analysis should be started as early as possible in the design of the data processing operation, even if some of the operational elements of the data processing are not known.
The continuous adaptation of the data management impact assessment/risk assessment throughout the project lifecycle will ensure adequate data protection and encourage solutions that facilitate GDPR compliance.

As the development process progresses, it may be necessary to repeat certain steps of the assessment because certain technical or organisational measures may have an impact on the severity or likelihood of the risks involved in the management of the data. Impact/risk assessment is an ongoing obligation, especially in cases where data management operations are subject to dynamic change.

The fact that the impact assessment procedure/risk assessment may need to be modified when data processing has actually started is not a sufficient reason to postpone or stop the assessment. Impact assessment/risk assessment is therefore not a one-off exercise, but an ongoing task.

A number of conditions must be taken into account to determine whether the Company is obliged to conduct a data protection impact assessment.

According to the GDPR (Article 35), an impact assessment is required in particular in cases where the envisaged processing may involve:

- a systematic and extensive assessment of certain personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions having legal effects concerning the natural person or similarly significantly affecting the natural person are based (e.g. systematic monitoring of employees' activities, including employees' workplace, internet activity, etc.)

- special categories of personal data referred to in Article 9(1) or the processing of a large number of personal data relating to decisions on criminal liability and offences referred to in Article 10;
- large-scale, systematic surveillance of public places (e.g.: collecting social media data to create profiles)

Note: Article 9(1) refers to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data and biometric data for the purpose of uniquely identifying natural persons, health data and data concerning the sex life or sexual orientation of natural persons.

The above list is not exhaustive, and depending on the circumstances, there may be additional "high" risk processing activities that are not included in the above list.

In general, the Company will decide whether a data protection impact assessment is required for a particular project, taking into account the list published by the NAIH and the existence of one or more of the following conditions:

a) personal data is shared with persons or organisations who have not previously had access to it;
b) personal data already processed are used for other purposes or in other ways;
c) new data management technology will be introduced;
d) automated decision-making/profiling;

Where it is not clear whether a data protection impact assessment is required for a particular project, it is recommended that one is carried out. The DPO, if any, can be consulted for clarification and the DPA can also be consulted. In all cases, the Management Board is entitled and obliged to take the decision (with the advice of experts) on whether or not an impact assessment is required or whether the Authority should be consulted.

The full context in which the impact assessment was carried out and an explanation of the reasons for the assessment should be recorded. The explanation should include the internal and external context of the project and its main objectives.

The scope of the study must also be precisely defined, which can be expressed in terms of the specific circumstances of the project, in particular:

- geolocation (e.g. country, office, data centre)
- organisational units (e.g. specific departments)
- business process (cause)
- IT service providers, systems or networks

- customers, products or services

Any exception must be justified in detail.

2.2.2 Documenting the use of personal data

Article 35(7)(a) to (b) of the GDPR states that the impact assessment shall include at least: a) a systematic description of the envisaged processing operations and a description of the purposes of the processing, including, where relevant, the legitimate interests pursued by the controller; and b) an assessment of the necessity and proportionality of the processing operations in the light of the purposes of the processing.

It must be demonstrated and documented in sufficient detail that the personal data used are relevant to the project, taking into account the following:

- Definition of the individual data elements stored and processed
- The reasons why the processing is absolutely necessary and proportionate - Purpose and legal basis of the processing
- How the data was obtained (source of data)
- How the data are processed (processing operations, operations carried out by processors)
- Duration of data processing
- How and where data is stored
- Possible future use of the data
- Data transmission
- Access to data

The information can be collected and presented through appropriate information registers, flowcharts and data access tools.

2.2.3 Risk identification

Identifying the risks to the personal data collected, processed and stored involves the following steps:

2.2.3.1 Identifying sources of risk

The following persons should be consulted when identifying risks:

The parties concerned (where possible):

- Manager(s) responsible for the activities concerned

- Staff actually carrying out the activity
- Service providers responsible for inputs to the activity
- Persons receiving the output of the activity
- Specific third parties with relevant knowledge
- Representatives of persons/organisations providing support and resources for the activity
- Other persons who can usefully contribute to the risk identification process

The risks identified should be recorded in as much detail as possible in order to assess the likelihood and impact of the risk.

2.2.4 Risk analysis

Risks to the rights and freedoms of data subjects, of varying likelihood and complexity, may arise from the processing of personal data, which may result in physical, material or non-material damage. In particular, the processing may result in:

- discrimination,
- identity theft or identity fraud, - financial loss, - damage to reputation ,
- the confidentiality of personal data protected by professional secrecy,
- undue influence on business decisions,
- the unauthorised removal of pseudonymisation,
- other significant economic or social disadvantage.

Damage can occur in different ways. Sometimes it can be tangible and quantifiable, such as financial loss or loss of a job. At other times it is less definable, such as the damage caused by the release of confidential or sensitive information to personal relationships and social situations. Sometimes the harm is not obvious, such as fear of identity theft, which may result in information security being compromised. The harm resulting from the use of personal information may be imperceptible to individuals and without consequence.

The likelihood and seriousness of the risk to the rights and freedoms of data subjects should be determined by reference to the purposes, nature, scope and circumstances of the processing.
When assessing the risks to data security, account should be taken of the risks posed by the processing of personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, or the transmission, storage or other processing of personal data in a way that could result in particular in physical, material or non-material damage.

The risk analysis provides numerical values for a) the likelihood and b) the impact/severity of the risk. By multiplying these values, it is possible to determine high and low risk ratings.

2.2.4.1 Evaluation of probability

An estimate of the likelihood of the risk must be made, taking into account whether the risk has occurred in the past in the organisation or in a similar organisation in the same economic sector or geographical location, and whether there is sufficient incentive, opportunity and capability for the threat to materialise.

The probability of each risk is ranked in numerical units from 1 to 5. General guidance on reporting numeric units is given in the following table. The assessment of the probability of risk should take into account information already available, internal control results. Depending on the subject of the risk assessment, more detailed guidance may be used for each level of probability.

Level	**Title**	**Description**
1	Unlikely	It never happened before, there is no reason to think it is more likely now
2	Not likely	It could happen, but it probably won't
3	Probably	Overall, the risk is more likely to arise than not to arise
4	Very likely	It would be surprising if the risk did not occur, given the frequency in the past and the present circumstances
5	Almost certainly	Either occurs regularly or is reasonably believed to be an imminent risk

The reasons for applying a given level should be recorded to facilitate interpretation and to allow for repeatability in future evaluations.

2.2.4.2 Risk impact/severity assessment

An assessment should be made of the impact of the risk on the rights and freedoms of data subjects and on the organisation. It should take into account existing effective controls that mitigate the impact.

Impacts should be considered in the following areas:

- Rights and freedoms of data subjects (mostly customers)
- Finance
- Health and Safety
- Good reputation
- Legal, contractual or organisational obligations

The impact of each risk should be marked on a numerical scale between 1 (low) and 5 (high). The following table provides general guidance for reporting all values.

Based on the scope of the risk assessment, it is possible to provide more detailed guidance for each level of impact.

The reasons for using a given level should be recorded to facilitate interpretation and to allow for repeatability in future studies.

Where appropriate, the data subjects or their representatives shall be consulted on the envisaged processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
Opinions may be obtained by various means and, depending on the circumstances (e.g. a general study on the purposes and means of the processing operations, a question to management representatives, or a standard survey sent to future customers), it must be ensured that the Company has an adequate legal basis for processing the data in respect of which the opinions are sought.
If the final decision on the processing differs from the opinion of the data subjects, the reasons for continuing or discontinuing the processing must be documented. It should also be documented if the Company does not seek the views of data subjects because it decides that it is inappropriate to do so, for example, if doing so would compromise the confidentiality of the Company's business plan or would be disproportionate or impracticable.

No.	Description	Rights and freedoms of data subjects	Consumer impact	Financial impact	Health and safety	Impact on reputation	Legal impact
1	Negligible	No effect, all rights and freedoms are guaranteed	No effect	None or very little	Very little additional risk	Negligible	No effect
2	Mild	Slight restriction	Certain local disruptions to normal business operations	Some	To an acceptable extent	Low	Small risk due to neglect of obligation
3	Moderate	Visible restriction of rights and freedoms, but for the purpose of the processing	It is still possible to deliver products/provide services with some difficulty	Undesirable but tolerable	High risk; requires immediate action	Moderate	The real danger of illegal operations
4	High	Unjustified interference with privacy	Severe business loss in key areas	Severe impact on revenue and/or profit	Significant risk to life	High	Illegal operation in some areas
5	Very High	The person concerned suffers damage	Economic collapse	Inability to function	Actual or highly probable death	Very High	Severe fines, damages and criminal consequences

2.2.4.3 Risk classification

Based on the assessment of the likelihood and the degree of impact/severity, a value is obtained by multiplying two numbers for each risk. The matrix shown in Figure 2 is used to decide the classification of the risk based on the value obtained.

All risks are classified according to the following values, as shown in the table below.

HIGH - 5 or more

LOW - 1-4

5	High	High	High	High	High
4	Low	High	High	High	High
3	Low	High	High	High	High
2	Low	Low	High	High	High
1	Low	Low	Low	Low	High
	1	2	3	4	5

The GDPR provides for an impact assessment procedure where the processing is likely to present a high risk to the rights and freedoms of natural persons, i.e. the GDPR distinguishes only between low and high risk. Accordingly, if the assessment of any of the processing operations is 5 or higher, an impact assessment must be carried out.

2.2.5 Risk assessment

The purpose of the risk assessment is to decide which risks are acceptable and which should be managed.

The matrix marked in the figure above contains the risk classification. The green colour indicates a risk below the acceptable limit. Areas in red generally indicate that the risk does not meet the risk acceptance criteria and therefore risk management will be required.

2.2.6 Definition of a risk management plan

For those risks that have been identified above as above the Company's threshold, solutions to mitigate the risks must be developed.

The general objective of risk management is to reduce the risk rating to an acceptable level. This is not always possible, because sometimes the value is reduced but the risk remains the same, e.g. a reduction from 8 to 6 still implies a high risk value. The organisation may decide to accept these risks despite the high risk level. Decisions of this type should be recorded with an appropriate explanation.

2.2.6.1 Risk management methods

The following methods may be used to manage risks that have been identified as unacceptable.

- Risk modification - the application of controls that reduce the likelihood and/or impact of a risk
- Avoiding risk by putting in place measures to ensure that the risk no longer exists
- Risk sharing with another partner (e.g. an insurer or supplier)

Decisions should be based on a consideration of the steps to be taken, which should be based on a sound knowledge of the circumstances of the risk. In particular

- Business strategy
- Regulatory and legal considerations
- Technical issues
- Commercial and contractual issues

2.2.6.2 Selection of controls

Appropriate controls should be defined to reduce the likelihood or impact (or both) of all risks to acceptable levels.

2.2.7 Risk assessment/impact assessment report

As a result of the assessment of the options for action, a risk assessment (and data protection impact assessment) report will be produced, detailing

- The proposed processing operations and a description of the personal data concerned
- The purposes of the processing, including, where applicable, the legitimate interests of the controller as defined in the GDPR
- The assessment of the necessity and proportionality of the processing
- The result of the assessment of the risks to the rights and freedoms of data subjects
- For each risk, whether it is recommended for acceptance or treatment - Priority order of risk management
- Risk managers
- Proposed risk management options
- Implementation of control(s)
- Responsible for the action to be taken
- Timetable of measures
- The level of residual risk after the controls have been carried out

The use of the program on the NAIH website (DPIA) to document the impact assessment report is recommended, but not mandatory.

2.2.8 Obtaining management approval for residual risks

At all stages of the data protection impact assessment, management should be informed of progress and decisions taken, including formal acceptance of the residual risk envisaged. Management approves the DIA report and considers the remaining risks and decides on any further action in the light of these.

Final approval shall be indicated in the manner prescribed in the Company's documents.

2.2.9 Prior consultation with the supervisory authority

Where the DIA indicates a high risk before the implementation of the identified controls, the GDPR requires that the supervisory authority must be consulted before the processing starts. The consultation should include the following information:

- details of the responsibilities of the controller, joint controllers and processors involved in the processing;
- the purposes and means of the intended processing;
- the applicable data protection controls;
- contact details of the DPO (if there is a DPO); - a copy of the impact assessment report;
- other information requested by the supervisory authority

If the Authority finds, in the course of the prior consultation, that the requirements laid down in the applicable law are not fully met in relation to the envisaged processing, in particular if it considers that the risks associated with the processing have not been adequately identified or mitigated by the controller, it shall, in addition to or instead of taking any other measures within its competence, determine the appropriate steps to remedy the deficiencies identified and propose to the controller or, limited to the scope of its activities, to the processor, the measures to implement them.
The Authority shall make its proposal in writing within six weeks of the initiation of the prior consultation. The Authority may extend this time limit by a maximum of one month, in which case it shall inform the controller or processor of the fact and the reasons for the extension within one month of the initiation of the prior consultation.

2.2.10 Application of risk management measures

Once the risk management plan has been adopted, the necessary measures should be monitored and implemented as part of the day-to-day monitoring of the project. If any of the measures are delayed or not implemented, the impact on the protection of the personal data concerned should be assessed and a decision on further action should be taken. If the unaddressed risk is serious, it may have a significant impact on the feasibility of the project.

2.2.11 Risk monitoring and reporting

Where possible, the effectiveness of risk controls should be measured and documented using objective indicators.

2.2.12 Regular review

The risk assessment should be reviewed annually and regularly to ensure that the assessments remain current and the findings and controls applied remain legally valid. Where necessary, an out-of-sequence risk assessment should also be carried out when changes in circumstances warrant it: e.g. in the event of significant business changes, mergers and acquisitions, changes in IT services/technology, etc.

2.2.13 Roles and responsibilities

The participants and their responsibilities in the risk assessment and control procedures are defined for each project individually, in line with the process described above. Where appropriate, a data protection expert may be involved with the approval of the management.

2.3. DATA MANAGEMENT RECORDS

All data controllers are required to keep a Data Management Register. Where the controller acts as a processor in a particular situation, the Data Processing Register shall contain data on the processing operations separately. The form of the Data Processing Register is set out in Annex 3 to this Code of Conduct. The Data Protection Contact Point (at the time of issuing this Code, Ms Antal Szontagh) is responsible for keeping the register.

2.4. THE DATA PROTECTION SYSTEM OF THE CONTROLLER

TASKS AND RESPONSIBILITIES OF ORGANISATIONAL ACTORS

2.4.1. DATA CONTROLLER

EWG Rail Private Limited Company is the controller of the data processing covered by the Policy.

Data relating to the Data Controller:

designation:	EWG Rail Private Limited Company
abbreviated name:	EWG Rail Ltd.
cégjegyzékszám:	01-10-049688
tax number:	26242387-2-41
Seats:	1134 Budapest, Róbert Károly körút 59.
e-mail:	info@ewgrail.com
phone number:	+36 1/866-3080

2.4.2. DATA PROTECTION OFFICER (DPO)

The controller and processor must appoint a data protection officer in the following cases:

- where the processing is carried out by public authorities or other bodies with public-service mission, except courts acting in their judicial role;
- where the main activities of the controller or processor involve processing operations which, by their nature, scope and/or purposes, require systematic and systematic large-scale monitoring of data subjects;
- where the main activities of the controller or processor involve the processing of a large amount of data relating to special categories of personal data within the meaning of Article 9 of the GDPR and to decisions on criminal liability and criminal offences referred to in Article 10.

The Data Protection Officer shall be appointed on the basis of professional competence and in particular expert knowledge of data protection law and practice, as well as suitability to perform the duties of Data Protection Officer.

The DPO may be an employee of the controller or the processor, or an external service provider under a service contract. In the case of an employee, the Company must ensure that the employee appointed as DPO is not involved in any step of the processing (independence), i.e. he/she cannot be a person

who determines the purpose, scope or necessity of the processing. The DPO may also perform other tasks. The controller or processor shall ensure that no conflict of interest arises from these tasks.

2.4.3 Decision-making procedure in relation to the employment of a Data Protection Officer

An internal analysis to determine whether or not the Company is required to appoint a DPO should be documented to demonstrate that relevant factors have been adequately assessed in the decision-making process, unless it is clear that the organization is not required to appoint a DPO. As with all privacy-related issues, this documentation should be updated, for example, when new activities or services arise that fall within the scope of the mandatory DPO case law.

2.4.4 The Company's current decision in relation to the employment of the Data Protection Officer

The Company is not a public authority or other body with public responsibilities and therefore Article 37(1)(a) of the GDPR does not apply. The core activities of the Company do not include the processing of large amounts of data relating to special categories of personal data under Article 9 GDPR and to decisions on criminal liability and criminal offences referred to in Article 10 GDPR, and therefore Article 37(1)(c) GDPR does not apply to it.

The main activity of the Company is rail freight transport. The Company processes only a limited amount of personal data and only in connection with its core business. Taking into account these facts and the above mentioned mandatory provisions, the management of the Company is of the opinion that the Company is not subject to the mandatory provisions and therefore it has been decided not to appoint a Data Protection Officer.

2.5. THE CONTROLLER'S OBLIGATION TO PROVIDE INFORMATION

The data controller is obliged to provide the data subject with information about the processing of his or her personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language.

2.5.1. Rules of procedure

There are two main ways of obtaining personal data, as set out in the GDPR:

a) the collection of personal data from the data subject (Article 13 GDPR)
b) obtaining personal data not from the data subject (Article 14 GDPR)

In both cases, the GDPR lists the information to be provided to data subjects. In addition, additional information may be provided. The following questions should be taken into account when drafting this Notice:

2.5.1.1 Does the data subject already have the information?

The GDPR requires that data subjects are informed of the information listed, unless the data subject already has this information. It is therefore important to establish that the data subject has all the information required to be provided and that this can be adequately verified.

If this is the case, the previous information should be documented and kept as evidence of compliance with the GDPR. The occurrence and verifiability of the information should be assessed individually for each data subject.

2.5.1.2 Where personal data is collected directly from the data subject

In cases where the data subject does not have the necessary information (for example, where data is collected on the website directly from users or employees), the following information must be provided at the time of collection of personal data:

- the identity and contact details of the controller and, if any, the controller's representative; - the contact details of the Data Protection Officer, if any;
- the purposes for which the personal data are processed and the legal basis for the processing;
- the legitimate interests of the controller or a third party;
- how the data is processed;
- where applicable, the recipients of the personal data and the categories of recipients, if any;
- where applicable, the fact and details of the controller's intention to transfer the personal data to a third country or international organisation,
- the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;
- information about the data subject's rights to request the controller to access, rectify or erase personal data relating to him or her, and the data subject's right to data portability
- information about the data subject's rights to request the controller to restrict the processing of personal data concerning him or her and to object to the processing of such personal data;
- information about the data subject's right to withdraw his or her consent at any time;
- information on the right of the data subject to lodge a complaint with a supervisory authority;
- whether the provision of the personal data is based on a legal or contractual obligation and the possible consequences of not providing the data;

- whether automated decision-making, including profiling, is taking place and, at least in these cases, the logic used.

2.5.1.3 *If the personal data is not* collected *from the data subject*

If the personal data has not been obtained from the data subject (for example, where the personal data is provided to the Company by a third party), there are a number of other circumstances (i.e. not counting the case where the data subject already has the information) where information does not need to be provided. These include:

- it proves impossible or would require disproportionate effort to provide the information in question,
- the acquisition or disclosure of the data is expressly required by Union or Member State law applicable to the controller, which provides for appropriate measures to protect the data subject's legitimate interests (Article 14 GDPR);
- personal data must remain confidential under an obligation of professional secrecy imposed by EU or Member State law.

Where any of the conditions apply, the reason for doing so must be properly documented and retained as evidence of GDPR compliance. Care should be taken to ensure that this is applied to all necessary information and all data subjects.

If none of the above conditions are met, the data subjects must be informed:

- within a reasonable time from the date of obtaining the personal data, but no later than one month;
- if the personal data is used for the purpose of contacting the data subject (e.g. email addresses) at least at the time of the first contact with the data subject;
- if the data are likely to be disclosed to other recipients, at the latest when the personal data are disclosed for the first time.

The following information should be provided:

- the identity and contact details of the controller and, if any, the controller's representative;
  - the contact details of the Data Protection Officer, if any;
- the purposes for which the personal data are intended to be processed and the legal basis for the processing; - the categories of personal data concerned;
- the recipients of the personal data or categories of recipients, if any;

- where applicable, the fact and details of the controller's intention to transfer the personal data to a third country or international organisation,
- the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;
- information on the data subject's rights to request from the controller access to, rectification or erasure of personal data relating to him or her, and the data subject's right to data portability
- information about the data subject's rights to request the controller to restrict the processing of personal data concerning him or her and to object to the processing of such personal data;
- information about the data subject's right to withdraw his or her consent at any time;
- information on the right of the data subject to lodge a complaint with a supervisory authority;
- the source of the personal data;
- whether automated decision-making, including profiling, is taking place and, at least in these cases, the logic used.

2.5.2 Information to the data subject

As with all information provided to data subjects in the context of the GDPR, it must be provided in a clear and easily accessible form, in clear and plain language. The best way to provide information to data subjects will depend on the specificities of the business process and may include the following:

- Notification on website
- By e-mail
- By printed letter/leaflet
- by phone

If the personal data are subsequently used for a purpose other than the one for which they were collected, the information to the data subject must be provided again in accordance with the new content before the processing for the different purpose can start.

The fact that the information has been provided must be properly documented so that it can be proven. This means that (i) if the information is provided on a website, it must be verified that the data subject has access to the full information and actively accepts it (ticks a box or presses the accept button, etc.), (ii) if it is provided by email, receipt of the email must be acknowledged, (iii) if it is provided by letter, receipt must be acknowledged, if it is provided (iv) in person, receipt must be acknowledged, and (v) in addition, the telephone call must be duly recorded.

Within the organisation, the person designated to approve the content of the information sheets is the CEO.

2.6. HANDLING OF REQUESTS FROM DATA SUBJECTS

The GDPR gives data subjects broad rights over their own data and it is important that the organisation is ready to ensure these rights are respected and requests are fulfilled in a timely manner.

2.6.1 General rules

Each request from a data subject is subject to the following general rules:

- Each piece of information must be provided to data subjects in a concise, transparent, comprehensible and easily accessible form, in clear and plain language, in particular for any information addressed to children;
- The information must be provided in writing or by other means, including electronic means where appropriate;
- At the request of the data subject, oral information may also be provided (e.g. by telephone or in person), provided that the identity of the data subject has been duly verified;
- We cannot refuse to comply with a data subject's request to exercise his or her rights unless we can prove that we are unable to identify the data subject;
- Without undue delay, but in any event within one month of receipt of the request, we must inform the data subjects of the action taken on the requests; if necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The extension of the time limit, stating the reasons for the delay, must be communicated to the data subjects within one month of receipt of the request;
- Where the data subject has made the request by electronic means, the information shall be provided by electronic means where possible, unless the data subject requests otherwise;
- If we do not take action on a request from the data subject, we must inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with a supervisory authority and to seek judicial remedy;
- We must provide information and action free of charge, unless a data subject's request is "manifestly unfounded or excessive, in particular because of its repetitive nature" (Article 12 GDPR). In these cases, we will charge an administrative fee for the costs or refuse to act on the request; the administrative fee is calculated as follows:

a) if the request does not require the provision of a medium or photocopying of paper documentation, the fee is HUF 3000 per hour.

b) if the data is provided on a data carrier, the charge for the data carrier + the charge under point (a)

c) if paper photocopying is required, an additional HUF 100 per page will be charged.

- If we have reasonable doubts about the identity of the natural person, we may request additional information necessary to confirm the identity of the data subject.

2.6.2 Steps of the procedure

Step by	**Description**	**Responsible**
Receipt of the data subject's request	The data subject may also make the request electronically (by e-mail or via our website), by post or by telephone. This can be accepted by any part of the organisation, but ideally it should be submitted via the helpdesk.	Receiving/receiving administrator
Logging of data subjects' requests	The fact and the date of receipt of the request must be recorded in the Register of *Requests from Data Subjects.* The identification data of the person making the request (name, address, other identification data), the type of request (deletion, correction, modification of data, etc.), the data concerned and the reasons for the request are also identified and recorded in the register. If the request is unclear, this must be indicated to the data subject without delay, together with information on the subject matter of the request.	Request Administrator
The person concerned proof of identity	The identity of the person concerned will be verified in accordance with the internal procedure depending on the way in which the request is made. If necessary, additional information may be requested to verify identity. If the data subject is not able to prove his or her identity, the request will be rejected and the reasons will be communicated to the data subject without delay and at the latest within one month of receipt of such a request.	Request Administrator

Assessment of the validity of the application	The test to determine whether the request is "manifestly unfounded or excessive" should be applied. This should be done by checking the Register of Requests from Data Subjects to see whether the applicant has made a similar request before and assessing the type of request. If so, a decision will be taken to refuse the request or to grant it for an extra fee. In the case of a request for rectification, erasure, restriction of processing and objection to processing, a decision must be taken as to whether the request is reasonable and lawful. If not, the request shall be refused and the request shall be rejected without delay and within a maximum of one month from the date of receipt of the request we must inform the data subject of the decision and of the possibility to lodge a complaint with the supervisory authority and exercise his or her right to judicial remedy.	Request Administrator
Step by	**Description**	**Responsible**
Imposition of a fee	If a fee is imposed, the person concerned must be informed of the fact and be given the opportunity to decide whether or not to proceed. If the person concerned decides not to proceed, the request shall be rejected and the reasons for this shall be communicated without delay.	Request Administrator
Compilation of the information requested	If the request is valid and can be fulfilled, the relevant information must be collected according to the type of request. This will include planning how the requested operation (e.g. restriction or erasure of processing) can be carried out. The request must be complied with within a maximum of 1 month, which may be extended by a further 2 months. The extension shall be notified to the data subject within one month of receipt of the request, stating the reasons for the delay.	Request Administrator / Data owner
Do the requested action / provide the requested information	The requested operation must be carried out (where possible) and the information requested must be sent to the data subject by electronic means, if he or she so chooses, or in writing by post.	Request Administrator

Closure of the data subject's application	The fact and manner of replying to the request (fulfilment/refusal) must be logged in *the Register of Requests of Data Subjects* with the date of closure of the request.	Application administrator

A table to be used as a Register of Data Subject Requests is attached as Annex 4 to these Data Protection Rules.

2.6.3 Possible requests of the data subject

2.6.3.1 Right to withdraw consent

Where the legal basis for the processing is the data subject's consent (and there is no other legal basis, such as the performance of a contractual or legal obligation), the data subject has the right to withdraw his or her consent.

Before deleting the personal data of the data subject from processing, it must be confirmed that consent is indeed the legal basis for processing. If not, the request may be refused on the grounds that the processing is based on another legal ground and that the data subject's consent is not necessary. Otherwise, the request must be complied with. In all cases, the request must be assessed in detail and complied with to the fullest extent possible, and reasons must be given for any refusal (including partial refusals).

The controller must ensure that the data subject can withdraw consent at any time and must allow the withdrawal of consent in the same simple way as the giving of consent.

In most cases, consent can be given and withdrawn electronically, i.e. online (e.g. by deleting a profile), so this procedure will not be necessary.

Where the consent of a child is required (persons under 16 years of age), the person who has parental authority over the child must approve the granting or withdrawal of consent and the identity of this person(s) must also be verified and recorded in the Register of Data Subject Requests under 'Notes'.

2.6.3.2 Right *to information*

At the time of obtaining the personal data, the data subject must be informed of the fact, purpose, legal basis, scope of the data processed, the method, duration or criteria for determining the duration of the processing, the rules on data portability, the right to lodge a complaint with the supervisory authority.

In addition to the information, the data subject must be expressly informed of the possibility to exercise the right to object and the information must be clearly displayed and separated from any other information.

For information:

(a) be provided to applicants on the page where the vacancy notice is published, in accordance with the relevant data management notice;

b) to persons who establish an employment relationship or other employment relationship with the Data Controller, at the time of the establishment of the legal relationship, with the content of the relevant data management information;

(c) be provided to persons entering the territory of the Controller prior to entering the territory, in accordance with the content of the relevant privacy notice.

The information referred to in point (a) shall be made available on the website of the Data Controller in a concise, transparent and easily accessible form, in clear and plain language.
The information referred to in point (b) must be provided in electronic form at the time of the establishment of the relationship, and the person concerned must provide written proof of this in the form of a paper declaration.
The information referred to in point (c) shall be displayed by means of a notice or sign on the fence or access gate at the boundary of the area.

2.6.3.3 Right of *access of the data subject*

Data subjects have the right to receive feedback from us on whether their personal data is being processed and, if such processing is taking place, they have the right to access their personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom or with whom we have disclosed or will disclose the personal data, including in particular recipients in third countries or international organisations;
- the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;
- the data subject's right to obtain from us the rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of such personal data;
- the right to lodge a complaint with a supervisory authority;
- if the data were not collected from the data subject, any available information on their source;

- the fact that automated decision-making, including profiling, is taking place and information on the likely consequences for the data subject;
- if personal data are transferred to a third country or an international organisation, the data subject has the right to be informed of the safeguards applicable to the transfer.

Access to personal data must be ensured in such a way that the data subject is as far as possible prevented from becoming aware of the personal data of another person. An exception to this may be made for personal data which relate to both the data subject and another person.
The Data Controller may restrict or deny the data subject's right of access proportionate to the aim pursued, where such a measure is strictly necessary:

a) the effective and efficient conduct of investigations or proceedings involving the Data Controller, in particular criminal proceedings;
b) the effective and efficient prevention and detection of criminal offences;
c) the enforcement of penalties and measures against offenders;
d) the effective and efficient protection of public security;
(e) the effective and efficient defence of the external and internal security of the State, in particular national defence and national security; or
(f) to ensure the protection of the fundamental rights of third parties.

If the Data Controller refuses or restricts the data subject's right of access, it shall immediately inform the data subject in writing, stating the reasons for the measure, provided that the purpose of the restriction or refusal is not jeopardised. In the notification, the Controller shall specifically draw the attention of the data subject to the fact that he or she may exercise the right of access with the assistance of the supervisory authority. Where the data processed are stored or backed up in the form of audio or video recordings, the material shall be provided in its original form, and transcripts or extracts shall be sufficient only if the original recordings have been destroyed.

2.6.3.4 Right to rectification

At the request of the data subject, the competent administrator responsible for data processing shall correct inaccurate personal data relating to the data subject without undue delay. Taking into account the purpose of the processing, the data subject shall also have the right to request the completion of incomplete personal data, including by means of a supplementary declaration.
Where necessary, the Company will take measures to verify information from data subjects to ensure its accuracy before it is recorded (e.g. by consulting personal documents).

2.6.3.5 *Right to erasure ("right to be forgotten")*

At the request of the data subject, the controller or the DPO shall, without undue delay, delete the personal data of the data subject or a set of personal data specified by the data subject, provided that one of the following cases applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- the data subject objects to the processing on the basis of Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing on the basis of Article 21(2) of the GDPR;
- the personal data have been unlawfully processed;
- personal data must be erased in order to comply with a legal obligation under EU or Member State law;

Reasonable efforts must be made to ensure erasure in the event that the data is disclosed. This means that, taking into account the available technology and the cost of its use, the Company must take all reasonable steps to inform the controller of the personal data that the data subject has requested the controller to delete references to such personal data and copies and replicas of the personal data.

The Controller may not delete personal data despite a legitimate request, if the processing is necessary:

- to exercise the right to freedom of expression and information;
- to comply with a legal obligation;
- in the public interest in the field of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; - for the establishment, exercise or defence of legal claims.

It is likely that these decisions will need to involve the Company's Data Protection Officer, if any, and in some cases senior management of the Company.

2.6.3.6 Right to restriction of processing

At the request of the data subject, the competent administrator responsible for processing shall restrict processing if one of the following conditions is met:

- the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time that allows us to verify the accuracy of the personal data;
- the data processing is unlawful and the data subject opposes the erasure of the data and requests instead the restriction of their use;

- the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims;
- the data subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

The data subject who has restricted the processing must be informed before the restriction is lifted.

For each such request, the Company must decide whether the request should be granted. It is likely that these decisions will need to involve the Company's Data Protection Officer, if any, and in some cases senior management of the Company.

Where processing is restricted as set out above, such personal data, except for storage, may be processed only with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for important public interests of the Union or of a Member State.
(3) The competent administrator carrying out the processing shall inform the data subject at whose request the processing is carried out of the lifting of the restriction on processing in advance.

Obligation to inform recipients and processors

The Data Controller shall inform all recipients and processors of any rectification, erasure or restriction of processing of personal data to whom or with which it has communicated or transmitted the personal data, unless this proves impossible or involves a disproportionate effort.

2.6.3.7 *The* right *to data portability*
At the request of the data subject, the competent administrator responsible for the processing shall ensure the portability of personal data, provided that the following conditions are met:

a) the personal data have been provided to the Data Controller by the data subject;
(b) the legal basis for processing is consent or a contract between the data subject and the controller;
c) processing is carried out by automated means;
(d) the processing of personal data does not adversely affect the rights or freedoms of others.

In exercising the right to data portability, the Data Controller shall provide the personal data to the data subject in a structured, commonly used, machine-readable format (PDF/XML).

The data subject may request that the Controller transfers the personal data directly to another controller. The data subject may exercise this option only if it is technically feasible.

The Data Controller is also obliged to make personal data available on paper in order to facilitate the exercise of the right of access.
Services in this category require a minimum decision-making process for each case, and it is highly desirable that this process be automated.

2.6.3.8 The right to object

The data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data on the following legal grounds:

- 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;
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such purposes, including profiling, where it is related to direct marketing. If the data subject objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for those purposes.

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

If an objection has been lodged, the Company must justify the grounds on which the processing is based and suspend the processing until this is done. If the processing of personal data is for direct marketing purposes (including profiling), we have no choice but to stop the processing.

In the event of an objection, the Controller may no longer process the personal data, unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2.6.3.9 *Automated decision-making on individual cases, including* profiling

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 concerning him or her or similarly

significantly affects him or her and to object to human intervention where necessary. The data subject has the right to express his or her views and to challenge decisions.

There are certain exceptions to this right, which apply if the decision:

- necessary for the conclusion or performance of a contract;
- the law allows;
- is based on the explicit consent of the data subject.

When assessing this type of request, it must be determined whether the above exceptions apply in the specific case in question.

2.6.3.10. Right to redress

In the event of a breach of his/her rights in relation to data processing, the data subject may contact the Data Controller's customer service adatvedelem@ewgrail.com, who will investigate the complaint and, if justified, will initiate action with the Data Controller's CEO, otherwise the complaint will be rejected.

The Data Controller shall inform the complainant of the refusal in writing within 30 days of receipt of the request, stating the factual and legal grounds for the refusal. In the event of refusal of the request, the complainant shall also be informed of the possibility of judicial remedy and of recourse to a supervisory authority. The administrator of the controller shall keep a record of rejected applications.

If the data subject still has a grievance about the way the Data Controller handles his or her data, or if he or she wishes to contact the authority directly, he or she may lodge a complaint with the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, PO Box 9. E-mail: ugyfelszolgalat@naih.hu, website: www.naih.hu).

The data subject also has the right to apply to the courts for the protection of his or her personal data, which will rule on the matter out of turn. In such a case, the data subject is free to choose whether to bring the action before the courts for the place of residence (permanent address) or the place of stay (temporary address) (http://birosag.hu/torvenyszekek).
The data subject can contact the court of the place of residence or domicile at http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso.

2.7. DOCUMENT MANAGEMENT AND DISPOSAL RULES

The document management and disposal rules in force at the Company are set out in the current Document Management and Disposal Rules.

2.8. THE REQUIREMENT FOR DATA SECURITY

The Controller shall implement appropriate technical and organisational measures to ensure and demonstrate that the processing of personal data is carried out in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons. Including, where applicable:

a) the pseudonymisation and encryption of personal data;

b) the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;

c) in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;

(d) a procedure for the regular testing, evaluation and assessment of the effectiveness of the technical and organisational measures taken to ensure the security of processing.

In determining the appropriate level of security, explicit account should be taken of the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

The Data Controller shall implement appropriate technical and organisational measures to ensure the effective implementation of the principles set out in this Policy and to incorporate additional data protection safeguards into the data processing process.

The Data Controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for the specific purpose of the processing are processed. This obligation relates to the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. These measures should ensure in particular that personal data cannot, by default, be made available to an indeterminate number of persons without the intervention of the natural person.

A document containing personal data must not be left in a place where a third party can access it. Such documents shall also be locked away in offices or staff rooms where third parties other than the competent document handlers may be present.

In order to prevent the loss of manually processed personal data, original documents should only be released in the course of official business, in particular judicial proceedings or investigative procedures. Before release, a complete copy of the original documents shall be made for safekeeping in the competent department.

In the event of damage or destruction of personal data, attempts should be made to replace the damaged data as far as possible from other available data sources. The head of the department where

the damage occurred shall be responsible for the replacement of the damaged data. The competent data controller who contributed to the recording of the data shall be involved in the replacement of the data. The fact of the replacement shall be indicated on the replaced data.

The personal data processed by the Company is stored by the Company in electronic and/or paper form.

The Company uses appropriate organisational and technical measures to ensure the security of the data. In determining the appropriate level of security, we explicitly take into account the risks arising from the processing of personal data, in particular risks arising from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

Data stored in electronic form is stored on a dedicated server at the Company's headquarters or branch.

Email is hosted using O365, a service provided by Microsoft as the data processor.

Backups to local hardware are covered in the IT policy.

Additional organisational and IT security measures to ensure the security of electronically stored data are set out in the IT Policy.

Paper documents containing personal data are filed according to specific filing rules. Folders containing personal data are stored in a lockable cabinet at the Company's headquarters, which is opened and closed daily. The locker keys are kept in a lockable safe. Access to filing cabinets is determined by business department according to specific instructions.

Security measures for access to the branch are set out in the Facility Security Policy.

The Data Controller shall ensure the enforcement of data security requirements by means of these Rules and separate instructions and regulations. The Data Controller shall ensure that its employees and third parties acting on its behalf (in particular, data processors) are aware of the contents of this Policy and the separate instructions and regulations in force at any time and act in accordance with them.

2.9. SPECIFIC CASES OF DATA PROCESSING

2.9.1. Processing of employee data

The Data Controller shall inform all employees or other persons entering into an employment relationship about the processing of data related to their employment. The data subject shall declare in writing that he or she has been informed.

The data in the payroll and employment register can be used to establish the facts relating to the employee's legal status, to verify classification requirements, for payroll, social security administration and statistical reporting.

To the extent necessary for the performance of their duties, the payroll and employment records shall be managed by the Controller's employee responsible for personnel matters.

2.9.2. Manually processed personal data

The Data Controller shall take into account the state of the art when defining and implementing measures to ensure the security of the data. It should choose from among several possible processing solutions the one which ensures a higher level of protection of personal data, unless this would impose a disproportionate burden on the Company.

The following measures must be taken to ensure the security of manually processed personal data:

a) the documents held in the archives must be kept in a lockable, dry room equipped with fire and property protection equipment;

(b) only the competent administrators have access to documents in permanent active management, and personnel, payroll and labour files must be kept securely locked,

c) the archiving of records of data processing shall be carried out regularly, and archived records shall be sorted and archived in accordance with the relevant requirements.

The rules for access to the keys to the rooms or lockers referred to in point (b) shall be laid down by the Controller's Chief Executive Officer.

2.9.3. Personal data processed electronically

If the Data Controller processes personal data in an electronic system that can only be accessed by a registered, competent employee who is on the access list, the competent employee must log in to the system with an individual, secret password. Once the processing is completed, the user must log out of the system. The Data Controller shall be responsible for password-protected data processing in the system.

To avoid data breaches, it is the employee's responsibility to protect his or her individual password. Apart from the employee, the individual password can only be known by the IT staff responsible for the

development and operation of the data management software and by the CEO, if it is necessary for the performance of their tasks at the Data Controller.

The computers used for data processing may not be left unattended in a state suitable for data entry or retrieval.

The Data Controller may only use a data management system which registers the access to the system and from the recorded data it can be determined who recorded the data and when.

2.9.4. Rules on checks on employees

2.9.4.1. Postal items

Mail received at the workplace, if it is assumed to be personal - for example, "s.k." or the exact name of the addressee is indicated - must first be given to the employee. If a letter with such contents is nevertheless opened, it must be sealed and the date of opening and the name of the person who has knowledge of the contents must be indicated.

2.9.4.2.2 Checking the use of telephones

The mobile and fixed telephones provided by the Data Controller to employees may be used primarily for official purposes, with private use permitted on an occasional basis, subject to proportionate use of resources.

If the Data Controller as an employer wishes to monitor the use of the telephone by employees on the basis of its legitimate interest, this may only cover official use, the monitoring of private use is prohibited. As a general rule, the Data Controller shall ensure the presence of the employee during the check and shall proceed in accordance with the principle of gradualness. Before carrying out the inspection, the employer shall inform the employee of the circumstances of the processing. Where the employer's control relates to the control of the employee's call log, the telecommunications service provider must be requested to provide a detailed call log for the telephone number in question, in such a way that the last three digits of the telephone numbers in the call log are in an anonymous form, so that the employee can select his private calls. Only the employee concerned and the employer's authorised representative shall have access to this anonymised call list.

In the event that the employee returns the mobile phone used by him/her, either during the employment relationship or upon termination of the employment relationship, it must be ensured that any private data stored on the device, such as telephone numbers, messages, pictures, films, other data in any form and content, can be backed up by the employee and then deleted irretrievably. The employee must provide a written declaration of the removal of private content in the form and content set out in Annex 7 to these

Regulations. The device may be handed over to a third party only after the person responsible for the device release is satisfied that no private data is or can be found on it. The person conducting the procedure shall be bound by confidentiality obligations with regard to the private data disclosed and shall not disclose it or any information relating to it to third parties.

2.9.4.3. Privacy policy for the use and control of e-mail accounts

The e-mail account provided for work purposes is given to the employee by the Data Controller for official purposes and may not be used for private purposes.

The IT department of the Data Controller responsible for the secure operation of the IT systems is entitled to determine the storage capacity of the e-mail inbox, to limit the size and format of the files attached to the e-mail and to inform employees about the information related thereto by e-mail as necessary, but at least every six months. Employees must comply with these settings and any additional user rules set by the department.

The employee may open and use additional non-business e-mail accounts on the work computer, provided that such private use does not harm the business interests and reputation of the Data Controller.

The Data Controller, as the employer, may, on the basis of its legitimate interest, control the official correspondence of the employee in compliance with the provisions of this Policy. During the verification, the Data Controller shall, as a general rule, ensure the personal presence of the employee and shall act in accordance with the principle of gradualness. The verification shall be based on the results of a balancing of interests test prepared by the Controller. The employer exercising the right of control shall inform the employee in a documented manner, before the actual control starts, of the specific interest for which the control is to be carried out. The employee must notify the employer or the person acting on behalf of the employer if the e-mail contains personal data before viewing the content of the e-mail during the inspection. The Data Controller may inspect the content of e-mails relating to work-related tasks without restriction.

When the employer wishes to check the contents of the official mailbox - based on the staged control system - he is entitled to ask the IT department for a list of the letter headers in the first place. The list may include the addressee, subject of the mail sent to and from the mailbox, the duration of the sending or receiving of the mail, if additional information is required, and the name and size of any attached file. Once the list has been consulted, the employer may designate the mail to be delivered to the employee, who is entitled to refuse the request only if the mail is of a private nature. The employer may not know the content of private correspondence. In the case of private correspondence which is not prohibited, knowledge of the contents of the letter is not necessary for the purposes of any employment law

consequences which may be applicable to the employee. The employer is entitled to require the employee to delete such correspondence and the employee is obliged to comply with the request.

If the necessary official correspondence should be sorted out from the mailboxes at a time when the employee concerned is permanently away from the computer, the employee concerned may designate an employee who can do this for him/her by logging on to the mailbox. If this is not the case, the line manager may designate two persons who, when present together, may only retrieve from the mailbox the specified official mail, but who are bound by confidentiality obligations in respect of non-official mail, and may not disclose its contents or any information about it to the manager or to any other person.

If the employee is suspended from work, the employee's e-mail address must be made inaccessible (blocked) to the employee and other employees for the duration of the suspension or for a maximum period of three months from the termination of the employment relationship, and an IT setting must be implemented which informs the sender of the mail sent to the mailbox address in an automatic reply that:

-the mailbox is no longer in use, and

-if you wish to send a letter of official correspondence to the Data Controller, to which e-mail or postal address.

After this deadline, the e-mail account address must be made inactive, i.e. an IT setting must be put in place to prevent the account from receiving further mail.

In the above information, it is not possible to provide data or information on the reason for the termination of the use of the e-mail box, or whether the employment of the employee concerned has been terminated, and if so, the reason for the termination.

In addition to making the mailbox inaccessible or inactive, you are prohibited from using any setting that would forward mail to the mailbox to another e-mail address.

The worker must be given the opportunity to retrieve any private correspondence from his/her mailbox on his/her last day of work, but no later than five working days after that date. This saving may be checked by a designated employee only if the reason for termination of employment justifies it. In this case, the designated employee shall be bound by a duty of confidentiality with regard to the private data of which he/she becomes aware.

If the mailbox contains official correspondence of such a nature that it may be necessary for the performance of future tasks and the retrieval of the documents would cause disproportionate difficulties for the Data Controller, the mailbox may continue to be used after the private data have been retrieved and permanently removed, and the employee concerned shall be informed thereof. Only official correspondence may be processed in the mailbox in the future.

2.9.4.4.4 Data protection rules for the use and control of the Internet by employees

The primary purpose of the Internet connection provided to employees is to facilitate efficient work, and the private use of the service is allowed without prejudice to the business interests and reputation of the Data Controller and without disproportionate limitation of the capacity of the IT system.

The IT department of the Data Controller responsible for the secure operation of the IT systems is entitled to restrict the use of the Internet and to define the keywords that the IT system automatically rejects when accessing websites containing them. These rules are set out in the relevant internal rules.

If there are reasonable grounds to believe that the employee is using the Internet connection in violation of the above rules, the employer must, as a general rule, clarify the circumstances of the violation by means of a personal interview.

Should the above procedure fail, the employer may request the involvement of the IT organisation by providing the employer with a list of the websites accessed on the computer of the employee concerned. In this case, the legal basis for the processing is the legitimate interest of the employer, based on a balancing of interests test carried out by the employer. The employer is entitled, as a general rule, to check the list in the presence of the employee concerned and to process the informal data only to the extent and for the duration necessary, without being able to know or process them in detail, and only to comment on them to the extent necessary to establish the possible consequences under labour law.

2.9.4.5. Control of the employee's workstation

The area where the employee works, such as his desk drawer, cannot be checked for employment purposes. Where the need to carry out checks for other purposes arises, such checks may only be carried out if the relevant legal provisions allow it and the DPO has given his or her prior approval. In any case, the employee must be fully informed in advance of the processing that will take place in connection with the inspection.

2.10. ACCOUNTABILITY

2.10.1 General requirements for data management and processing.

A person who has a legal relationship with the Data Controller (personal scope) and who comes into possession of personal data or processes personal data on the basis of his or her job or position, shall protect and safeguard the personal data and shall make every effort to ensure their adequate protection.

The data must be protected, in particular against unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or accidental damage, and inaccessibility resulting from changes in the technology used.

Persons having a legal relationship with the Data Controller or persons acting on behalf of the Data Controller are obliged to treat confidentially all personal data that have become known to them in connection with their legal relationship.

Persons who have a legal relationship with the Data Controller and who carry out data processing or processing operations shall be liable for any damage resulting from a breach of their data processing or data protection obligations.

Where the processing is carried out on behalf of the Controller, the Controller may only use processors that provide adequate guarantees to implement appropriate technical and organisational measures to ensure compliance with the requirements of the processing and to protect the rights of data subjects.
The processing carried out by the processor shall be governed by a contract binding the processor to the Controller. The contract may only be concluded in writing.
The contract must specify in particular:

a) the identity of the Data Controller and the Data Processor;
b) the subject of the processing;
c) the type of personal data to be processed;
d) the amount of personal data to be processed (if possible);
e) the categories of persons concerned;
f) the nature and purpose of the processing;
g) the legal basis for the processing;
h) the duration of the processing;
i) what to do when the provision of the processing service is terminated;
j) the obligations and rights of the Data Controller;
(k) the processor processes the personal data solely on the basis of the controller's written instructions, including the transfer of personal data to a third country or an international organisation, unless the processing is required by Union or Member State law applicable to the processor, in which case the processor shall notify the controller of that legal requirement prior to the processing, unless the notification of the controller is prohibited by the relevant legislation on grounds of important public interest;
(l) the way in which instructions are given to, or contacts are maintained between, the Controller and the processor;
(m) the decision to use an additional processor;
n) the processor respects the legal requirements for the use of an additional processor;
o) confidentiality;
p) data security requirements;

q) assisting in the enforcement of data security standards, incident management and impact assessments;
r) assisting in the exercise of the rights of the person concerned;
(s) the provision of information to the Data Controller and the Data Controller's right of control;
t) the method of carrying out the control of the Data Controller;
u) certain liability issues;
v) the means of enforcement.

Where necessary, the controller and the processor shall take additional measures to ensure that natural persons who have access to personal data and who act under the authority of the controller or the processor process those data only in accordance with the controller's instructions.

2.10.2. Requirements for data transmission

Within the organisational system of the Data Controller, personal data may be transferred - to the extent and for the period necessary for the performance of the task - to an organisational unit or person whose knowledge and processing of the personal data is necessary for the performance of the task performed by the Data Controller.

Data processing for different purposes may be combined by the Data Controller only in accordance with legitimate purposes and where justified.

A request for the transfer of personal data processed by the Data Controller may only be fulfilled on the basis of a legal requirement or if the conditions set out in the following paragraph are met. In all other cases, the transfer shall be refused.

In cases where the transfer is not based on a legal obligation, the request may only be complied with if the data subject gives his or her consent, after having been informed in detail, in a verifiable manner, or if it is necessary for the purposes of the legitimate interests pursued by the Data Controller or a third party.

In the case of data transfers abroad, the data exporter must specifically verify that the conditions for data transfers abroad set out in the GDPR are met. This should include an assessment of whether the transfer is in accordance with one of the legal bases set out in the GDPR and whether an adequate level of data protection is ensured by the receiving controller. If the transfer is to a Member State of the European Economic Area, the adequate level of protection of personal data does not need to be assessed.

Transfers of personal data, including retransfers of personal data from a third country or international organisation to another third country or another international organisation, which are or are intended to

be subject to processing following their transfer to a third country or international organisation, may only take place if both the controller and the processor comply with the conditions set out in the GDPR.

A transfer of personal data to a third country or an international organisation may take place if the European Commission has determined or published in the Official Journal of the European Union and on its website that the third country, a territory or one or more specific sectors of a third country or the international organisation in question ensures an adequate level of protection (adequacy decision). No specific authorisation is required for such transfers.

When transferring personal data by postal mail, you must ensure that the mailing is sealed.

The Data Controller undertakes to provide personal data for statistical purposes only in such a way as to ensure that it cannot be linked to the data subject.

The Data Controller shall keep a record of the data transfers made by it in accordance with the register in Annex 6 to the Rules.

2.10.3. Records of processing activities

The Controller shall keep records of all its processing activities which:

(a) is likely to result in a risk to the rights and freedoms of data subjects;
b) not of an occasional nature;
c) involves the processing of sensitive data or personal data relating to criminal offences.

The Data Controller shall comply with the above record-keeping obligation in accordance with the content of Annex 3 to this Privacy Policy.
The administrator carrying out the processing shall fulfil the obligation to keep records on behalf of the Data Controller in accordance with this point.
The CEO will ensure that the records of data protection activities are kept up to date.

The Executive Director shall make the register available to the NAIH upon request.

Records of data protection activities include:

a) the name and contact details of the Data Controller;
b) the description of the processing;
c) the actual place of processing;
d) the purpose of the processing;
e) the legal basis for the processing;
f) the legal basis for the processing;
(g) in the case of joint processing, the name and contact details of the joint controller;
h) the place of processing;

(i) the activities of the processor in relation to the processing;
j) the technology of data processing;
k) the name of the IT application;
l) the scope of the personal data processed by the controller;
m) the duration of the processing;
n) the source of the data;
(o) in the case of a transfer, the type of data;
p) the name and contact details of the recipient;
q) in the case of transfer of personal data to a third country or an international organisation, information on the appropriate safeguards;
r) the legal basis for the transfer;
s) the scope of the stakeholders;
t) a description of the technical and organisational measures taken to ensure data security.
IX.

2.11. ORGANISATION OF INTERNAL TRAININGS, GDPR TRAININGS AND DEVELOPMENT OF DATA PROTECTION AWARENESS IN THE WORK ORGANISATION, REGULAR INTERNAL DATA PROTECTION AUDIT PROCESSES

In line with the requirement of data-conscious organisation, the Company places great emphasis on the importance of data protection principles and rules in all areas of its operations and to raise awareness of these within the organisation. According to Article 39 of the GDPR, the DPO shall monitor compliance with the GDPR and other EU or Member State data protection provisions and the controller's or processor's internal rules on the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in data processing operations, and related audits. Where a DPO is not appointed, the Company will organise the necessary education/training to raise the awareness of staff.

2.11.1 Internal training structure

In order to increase data protection awareness, the Company applies the following training and knowledge reporting system for its colleagues who carry out data processing operations as part of their job.

2.11.1.1.1. Privacy training on entry

Within 10 days of joining the Company, you will be provided with mandatory training on data protection awareness, including the following mandatory topics: the concept of personal data, the concept and legal basis of data processing, data protection risk, risk assessment, data awareness in everyday business, the obligation to report incidents, the main data processing activities of the Company.

2.11.1.2.2. Annual data protection awareness training

Attendance at at least one centrally organised data protection awareness training session once a year is mandatory for all colleagues who handle personal data. The training can be organised in-house, but it is also possible to use an external provider.

2.11.1.3. Annual test to measure data protection preparedness

Within 14 days of attending the annual mandatory presentation, all colleagues who have personal data must provide an online test of their data protection knowledge. The test will be considered successfully completed if the colleague achieves a score of at least 80%. Accordingly, the test must be completed until the 80% requirement is reached.

2.11.2 Other provisions

The Company will review and update the training materials and the data protection knowledge test on which the data protection training system is based, on an annual basis, centrally, under the coordination of the Data Protection Officer (if any) and, if necessary, with the assistance of an expert, in accordance with Article 39 (1) (b) GDPR.

2.12. DATA BREACH HANDLING

A data breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A data breach may cause physical, pecuniary or non-pecuniary damage to the data subjects (and indirectly to the Company) if not addressed in a timely and appropriate manner. Such damage may include, but is not limited to, loss of control over their personal data (where unauthorised persons gain access to the data and there is no way of knowing what it will be used for), financial loss (e.g. theft of credit card data), damage to reputation, leakage of proprietary business information, etc.

Examples of the most common incidents include: loss of laptop, mobile phone, data media containing personal data, sending personal data to the wrong email address, unsecure storage of personal data (e.g. payment slips thrown in the trash); unsecure transmission of data, unauthorised copying or transmission of customer and partner lists, server attacks, website hacking.

2.12.1. Detection of a data breach

The Data Controller may be notified of the unexpected event either by internal or external signal.

An internal signal is deemed to be an unexpected event if a person in an employment or other legal relationship with the Data Controller or a data processor acting on the basis of a contract with the Data Controller becomes aware of the unexpected event.

If a person in an employment or other legal employment relationship with the Data Controller notices the unexpected event, he/she shall inform his/her immediate superior or the head of the Data Controller without delay, but within 2 hours of the discovery.

If a person in an employment or other employment relationship with the Data Controller becomes aware of the unexpected event, who does not have a direct superior, he or she shall inform the head of the Data Controller without delay, but no later than 2 hours after the discovery.

If a data processor acting under a contract with the Data Controller becomes aware of the unexpected event, he or she shall inform the Data Controller's manager through the contact person specified in the said contract without undue delay, but no later than 2 hours after the discovery.

An external indication is deemed to be a notification if any person other than the persons defined above becomes aware of the unexpected event and informs the Data Controller orally, in writing or electronically.

If the external signal is received by a person who has an employment or other legal employment relationship with the Data Controller, that person shall inform his or her immediate superior or the head of the Data Controller without delay, but no later than 2 hours after the detection.

If the information is received by a person who is employed by the Data Controller or has another employment relationship with the Data Controller and who does not have a direct superior, the person shall inform the head of the Data Controller without delay, but within 2 hours of the discovery.

If the information is received by a processor acting under a contract with the Data Controller, the processor shall inform the Data Controller's manager through the contact person specified in the said contract without undue delay, but no later than 2 hours after the detection.

Any request sent by the NAIH to the Data Controller shall be considered as an external signal.

The head of the controller must examine without delay any information received about an unexpected event. In doing so, it shall take into account the following factors:

- whether the unexpected event involves personal data;

- whether the unexpected event was caused by a breach of security;
- what the result of the breach of security was for the personal data.

In the context of the investigation of the unforeseen event, the head of the Data Controller shall be entitled to request information from the person employed by the Data Controller, from any other person having an employment or other legal relationship with the Data Controller, and from the data processor acting under a contract with the Data Controller.

If, as a result of the investigation carried out, the Data Controller's manager establishes that an unforeseen event affecting personal data has occurred as a result of a breach of security, this shall be considered to be a coming to the knowledge of the Data Controller within the meaning of Article 33(1) of the GDPR.

If, as a result of the investigation, the Data Controller's manager determines that the unexpected event constitutes a data breach, he or she must also categorise the incident.

2.12.2. Investigation of the data breach

The Head of the Data Controller shall convene the Incident Management Team without undue delay, but no later than 2 hours after becoming aware of the incident.

The Incident Management Team is responsible for investigating the circumstances of the data breach, assessing, analysing and managing the risks of the data breach and deciding on further action to be taken in relation to the data breach.

The Incident Management Team is led and managed by the Head of the Data Controller.

The Incident Management Team shall meet on a regular basis, as determined by the Head of the Data Controller, until the handling of the data protection incident is completed.

The Incident Management Team will be terminated upon the conclusion of the handling of the data protection incident, including any decisions taken in the framework of the NAIH procedure.

At the end of its activities, the incident management team shall prepare a report to the Data Controller's executive manager on the handling of the incident in the form and content set out in Annex 8 to these Rules.

Members of the Incident Management Team:

- IT Director;
- the legal representative of the company;
- a colleague of the person concerned;

- the CEO of the Controller or a person appointed by the CEO.

The incident management team may include other persons as necessary.

The first meeting of the Incident Management Team is opened by the Head of the Data Controller.

At the first meeting of the Incident Management Team, the Data Controller's Head shall present the available information and facts about the data breach, in particular the circumstances in which the data breach occurred and the categorisation of the data breach.

The Incident Management Team will then start assessing and analysing the risks of the incident, taking into account their likelihood and severity. The risks should be considered in terms of their source, the serving environment, the personal data and the potential impact of the incident.

(4) Factors that may be taken into account as to the source of the risks:

a) the incident is the result of unintentional internal conduct or activity;
b) the incident is the result of intentional internal conduct or activity;
c) the incident is the result of unintentional external behaviour or activity;
d) the incident is the result of intentional internal conduct or activity.

(5) Factors to be taken into account for the serving environment:

a) the means of data processing (paper-based or automated);
b) the system involved in the incident (mail system, storage media, etc.);
c) measures to protect the security of the server environment (e.g. encryption, naming, firewall);
d) the resilience of the serving environment;
e) the effectiveness of the measures taken in advance to deal with the incident;
f) the factors that allowed the incident to occur;
g) other factors influencing the occurrence of the incident;
h) the likelihood of restoring systemic functioning.

(6) Factors that may be taken into account for personal data:

a) the categories of personal data, in particular sensitive data;
b) personal data number;
c) the categories of persons concerned, in particular their vulnerable situation (children, workers);
d) the identity of the data subjects;
e) the number of people concerned.

(7) Factors to be taken into account for the impact of the incident:

a) physical damage or danger;
b) property damage;
c) non-pecuniary damage.

The incident management team is required to classify the incident individually according to the risk level, as follows: low, medium or high risk incident.

A high number of cases under paragraph 4(b) to (d), of vulnerable data subjects under paragraph 6(a) and (c), of personal data subjects under paragraph 6(b) and of data subjects under paragraph 6(e) shall be considered as medium or higher risk.

There is also likely to be a higher risk to the rights and freedoms of natural persons if a data breach results in:

a) discrimination against the person concerned;
b) identity theft;
c) identity theft;
d) financial loss;
e) damage to the reputation of the person concerned;
f) breach of the confidentiality of personal data protected by professional secrecy;
g) unblocking pseudonymisation without authorisation;
h) any other significant economic or social disadvantage;
i) an inability to exercise your fundamental rights or freedoms;
j) the loss of the right of data subjects to exercise their own choices with regard to their personal data;
k) evaluate personal characteristics for the purpose of creating or using a personal profile.

Where the data breach is low risk, it is considered unlikely to pose a risk to the rights and freedoms of natural persons.

Where the data breach is of medium risk, it is considered to be likely to result in a risk to the rights and freedoms of natural persons, as referred to in Article 33(1) of the GDPR.

Where a data breach is considered high risk, it is deemed to be likely to result in a high risk to the rights and freedoms of natural persons, as referred to in Article 34(1) of the GDPR.

The incident management team is also required to take all necessary measures to mitigate or prevent the consequences of the data breach, including restoring the functioning of the systems concerned, informing the data subjects, if any, and, in the event of a breach or crime, notifying the authorities competent and competent to investigate the breach or crime.

2.12.3. Reporting a data breach

Where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Data Controller shall notify the NAIH without undue delay and, if possible, no later than 72 hours after becoming aware of the personal data breach.

If the circumstances of the data protection incident and the assessment of the risks justify it, the notification may be made in instalments.
On behalf of the Data Controller, the obligation to notify shall be fulfilled by the Chief Executive Officer. The Executive Director will make a notification on paper or via the electronic notification system available on the NAIH website.

The notification to the NAIH must include:

a) the Data Controller's data;
b) the date of the data breach;
c) the date of becoming aware of the data breach;
d) how the data breach was detected;
e) the reasons for any delay in providing information;
f) the nature of the data breach;
g) personal data affected by the data breach;
h) the estimated number of personal data affected by the data breach;
i) the categories of persons concerned;
j) the measures taken before the data breach;
k) the consequences of the data breach;
l) physical, material or non-material damage or other significant consequences for the data subjects and the seriousness of the likely consequences;
m) the measures taken;
n) the measures taken to remedy the data breach;
o) other notifications;
p) the name and contact details of the Data Protection Officer.

All employees of the Data Controller are obliged to cooperate with the NAIH in the proceedings initiated in connection with the handling of data breaches.

The Executive Director is obliged to provide the NAIH with any additional information necessary for the conduct of proceedings in connection with the handling of data breaches.

In order to fulfil the above obligation, the CEO is entitled to request information from the person having an employment or other legal employment relationship with the Data Controller, as well as from the data processor acting on the basis of a contract with the Data Controller.

Members of the incident management team must cooperate with the DPO in fulfilling this obligation.

If the notification is not made, the Data Controller shall document the reasons for not making the notification.

Information on whether or not a report has been made will be part of the incident management team's report.

2.12.4. Information to data subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the personal data breach without undue delay.

The Data Protection Officer shall fulfil the obligation under paragraph 1 on behalf of the Controller.

Where the personal data breach concerns persons employed by the Data Controller, the information shall be provided through the systems used for the purpose of contacting the employees, with the involvement of the departments employing the data subjects.

Where the personal data breach involves persons not covered by paragraph 3, the information shall be provided by means of the systems used to communicate with the data subjects. In this case, the Controller's press relations officer shall assist in the development of the content of the information.

Where, in view of the large number of data subjects, personal information would be impossible or disproportionately burdensome for the Data Controller, the information may also be provided by means of a notice in the local or national press.

In the cases referred to in the previous two paragraphs, an alert notice shall be placed on the website of the Data Controller providing general information on the nature of the incident, the personal data concerned and the category of data subjects.

The information provided to the data subject or data subjects shall include at least:

a) a description of the nature of the data breach;
b) the name and contact details of the Data Protection Officer;

c) a description of the likely consequences of the data breach;
d) a description of the measures taken or envisaged to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the breach;
e) a description of the measures that the data subjects can take to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the breach.

In order for the CEO to fulfil his/her duty to provide information, he/she is entitled to request information from the person having an employment or other legal employment relationship with the Data Controller, as well as from the data processor acting on the basis of a contract with the Data Controller.

Members of the incident management team must cooperate with the CEO in fulfilling the duty to inform.

If information is not provided, the reasons for not providing it must be documented by the CEO.

Information on whether or not information has been provided will be part of the incident management team's report.

2.12.5. Recording of the data breach

The Data Controller is obliged to keep records of data breaches, regardless of their risk classification. The Data Controller shall comply with its obligation under the previous paragraph in the form and content set out in Annex 9 to this Policy.
Data protection incident records include:

a) the name and contact details of the Data Controller;
b) the identifier of the data breach;
c) the scope of the personal data concerned;
d) the data subjects affected by the data breach;
e) the number of people affected by the data breach;
f) the date on which the data breach occurred;
g) the date on which the data breach became known;
h) the nature of the data breach;
i) the circumstances of the data breach;
j) the impact of the data breach;
k) the measures taken to respond to the data breach;
l) other data specified in the legislation providing for the processing;
m) the fact of the obligation to notify;
n) the date of the official notification;
o) the name of the person making the notification;
p) the fact of the obligation to inform;

q) the date on which the data subjects were informed;

r) the date of the entry.

The Chief Executive Officer shall carry out the registration obligation on behalf of the Data Controller. The CEO shall ensure that the records of data protection incidents are kept up to date and updated. The Executive Director shall make the register available to the NAIH upon request.

2.13. INTERNAL RULES TO BE FOLLOWED IN THE EVENT OF ACTION BY THE DPA

The Chief Executive Officer (the person responsible) is primarily responsible for ensuring proper cooperation with the Authority within the Company's organisation. Any request from the Authority must be forwarded by the responsible person to the CEO immediately upon receipt of the request. the CEO, in consultation with the Company's legal representative, may, if necessary, depending on the nature of the request, initiate the setting up of an internal working group or the involvement of an external expert. In all cases, you must respond to the Authority's request within the prescribed time limit, enclosing all data/information/documents requested by the Authority. The content of any document to be sent to the Authority shall be approved by the Executive Director.

1. Annex 1 - Interest Assessment Test form

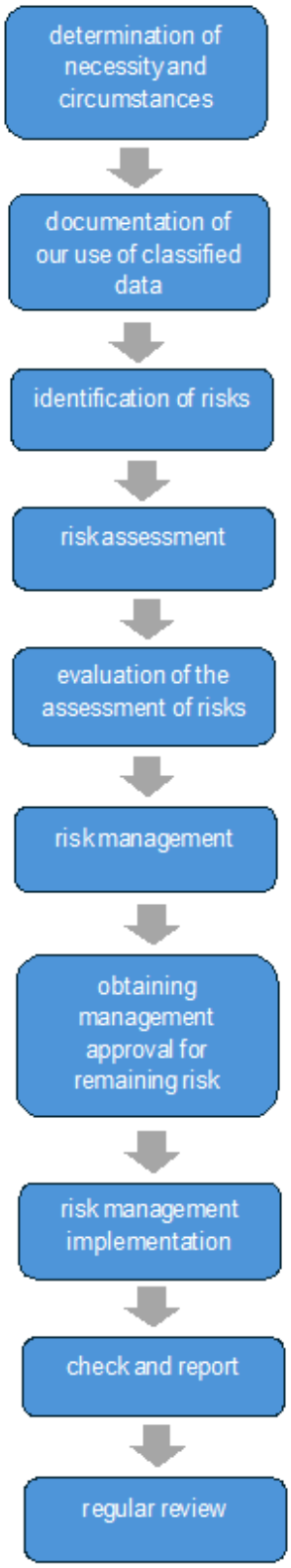
INTEREST ASSESSMENT TEST	
Company name	
Subject of the interest test	
Prepared by (name, job title)	
Approved by (name, job title)	
Date of preparation	
Date of approval	
Log number	
Purpose of the envisaged processing	
Legal basis for the envisaged processing (GDPR compliance)	
Scope of the personal data concerned by the processing	
Source of personal data	
Duration of processing	
Guarantees given by the Company	
FINDINGS	

The legitimate interest of the Company	
Necessity of the processing	
Violation of the rights and freedoms of data subjects	
Balance of interests	

Done at: Budapest, 20.....

CEO

2. Annex 1 - Risk assessment process



3. Annex 1 - Data Management Register

THE PROCESSING ACTIVITIES

Name of data processing	
Actual place of processing[1]	
Purpose of data processing[2]	
Legal basis for data processing	
Name of the legal basis for processing	
Name, address of the joint controller[3]	
Place of processing[4]	
Processor's activities in relation to data processing[5]	
Technology for data management[6]	
Name of the IT application	
Scope of personal data processed by the controller[7]	
Duration of processing	
Source of data[8]	
Type of data in case of data transmission[9]	
Name of the addressee, full address[10]	
Information on the appropriate safeguards in case of transfer of personal data to a third country or an international organisation[11]	
Legal basis for the transfer[12]	
Who is affected[13]	
Description of the technical and organisational measures taken to guarantee data security[14]	

[1] The address of the Data Controller (if the data are stored in a different location, please provide this).
[2] What is the purpose of this data?
[3] Article 26 GDPR.
[4] Where the data is recorded or stored.
[5] If there is a data processor, you must specify what activity they perform. For example: hosting, mailing, website maintenance.
[6] Manually or by electronic information system (IT application, electronically).
[7] For example: name, mother's name, address, e-mail address, etc.
[8] Is the data coming from the data subject or from a 3rd person or organisation?
[9] In the case of data transfer, when data goes outside the company, what data goes (specifically named as in point 9)
[10] The name of the data processor to whom the data is transferred must also be included here.
[11] Does personal data go to a third country (outside the EU)? And why (please specify)?
[12] E.g. consent, contract.
[13] Elderly, relative, beneficiary, contact person, clients.
[14] Name of data security measures applied

Name of data processing	
Actual place of processing	
Purpose of data processing	
Legal basis for processing	
Name of the legal basis for processing	
Name, address of the joint controller	
Place of processing	
Processor's activities in relation to data processing	
Technology for data management	
Name of the IT application	
Scope of personal data processed by the controller	
Duration of processing	
Source of data	
Type of data in case of data transmission	
Recipient name, full address	
Information on the appropriate safeguards in case of transfer of personal data to a third country or an international organisation	
Legal basis for the transfer	
Who is affected	
Description of the technical and organisational measures taken to guarantee data security	

Name of data processing	
Actual place of processing	
Purpose of data processing	
Legal basis for processing	
Name of the legal basis for processing	
Name, address of the joint controller	
Place of processing	
Processor's activities in relation to data processing	
Technology for data management	
Name of the IT application	
Scope of personal data processed by the controller	

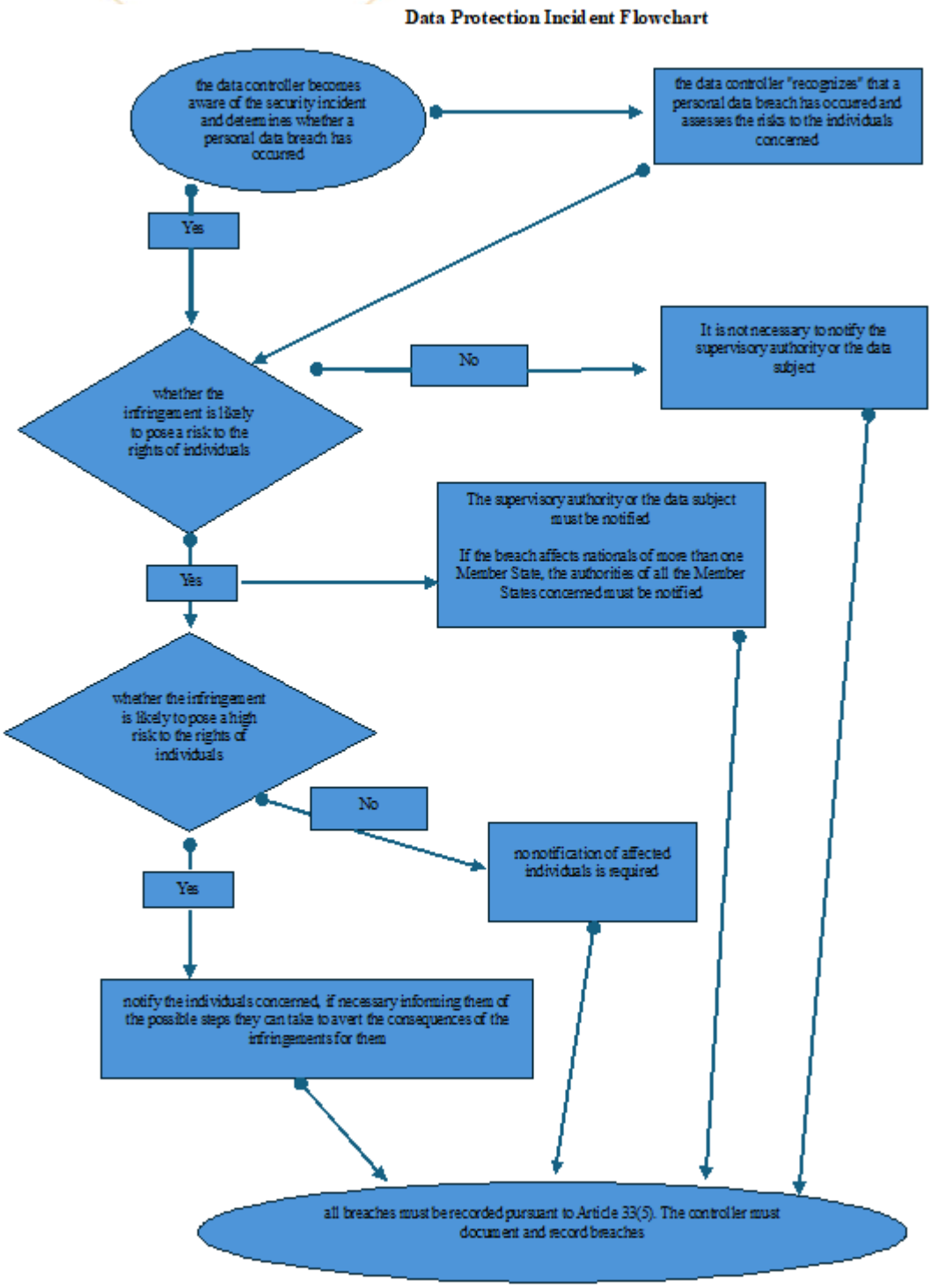
Duration of processing	
Source of data	
Type of data in case of data transmission	
Name of the addressee, full address	
Information on the appropriate safeguards in case of transfer of personal data to a third country or an international organisation	
Legal basis for the transfer	
Who is affected	
Description of the technical and organisational measures taken to guarantee data security	

4. Annex 1 - Privacy Policy

REGISTRATION OF DATA SUBJECTS' REQUESTS

	Name and contact details of the data subject who wishes to exercise his or her right of access	Nature of the right of access sought (content of the request)	Date of the request for enforcement	Legal basis for the processing of data of a data subject who wishes to exercise his or her right of access	Action taken to comply with the enforcement request	Date of execution of the enforcement request	Legal and factual grounds for measures restricting or refusing access rights	Date of registration, signature of the registrar
1.								
2.								

5. **Annex 1 - Data Protection Incident Flowchart** (Source: Data Protection Working Party - WP250rev01 - Guidelines)



6. Annex No.

THE RECORDING OF DATA TRANSMISSIONS

№	Date of transmission of personal data	Name of the reporting department	Legal basis and purpose of the transfer	Definition of the scope of personal data transferred	Recipient of the transfer	Transfers to third countries	Other data specified in the legislation providing for the processing, additional remark	Date of entry, name of registrant, signature
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								

7. Annex No.

Declaration of the data content of the IT equipment when it is returned

Name: ....., (mother's name :....., place of birth:....., date of birth:.....) I declare that EWG Rail Private Limited Company (1134 Budapest, Róbert Károly körút 59.; tax number: 26242387-2-41) as my employer has provided me with the following infocommunication devices (work computer, smartphone, other IT and infocommunication devices) for the purpose of performing the tasks related to my job

name of the device: ID:

.....

.....

.....

.....

I declare that the above tools contain only data related to my work tasks.

Cd: .....,.....

.....

employee

I have received the declaration on behalf of EWG Rail Private Limited Company:

Cd: .....,.....

.....

Name signature

Annex 8

PROTOCOL

DATA BREACH HANDLING

Conference details	
Name and purpose of the meeting:	**Data Protection Committee, data breach investigation**
Date and location:	
Protocol number:	
Keeper of the minutes:	
Names of participants	**Participants' job titles**

1. **Background:**

2. **Classification of the event**

- On the basis of the above, it can be concluded that a data protection incident has/has not occurred, (reason: ...)

3. **Data breach characteristics:**

- The nature of the stakeholders:
- The number of people affected:
- Nature of injury:
- Nature of the data breach:
- Reason for data breach:
- The circumstances and effects of the data breach:
- Description of the measures taken before the data breach:
- The consequences of a data breach:
- The nature of the personal data concerned:

4. Findings and proposals

In view of the nature and seriousness of the data breach and its consequences and adverse effects on the data subject, the Data Protection Committee has decided that a notification to the Data Protection Authority is/is not necessary and that the data breach poses a high risk to the rights and freedoms of data subjects, i.e. their privacy.

5. Data Protection Committee proposals:

a) ...
Responsible: ...

b) In the area of risk mitigation:
Responsible: ...

c) Other
Responsible: ....

d) Deadline for action taken:...

Date:

.....	.....	.....
name, job title	name, job title minute-taker	name, job title

.....
name, job title

Annex 9 - Data Protection Incident Register

DATA BREACHES

Serial number[15]	
Scope of the personal data concerned[16]	
Data subjects affected by the data breach[17]	
Number of data subjects affected by a data breach	
Date of the data breach	
Date of becoming aware of the data breach	
Nature of the data breach	
The circumstances of the data breach	
Impact of the data breach	
Measures taken to respond to the data breach	
Other data specified in the legislation providing for the processing	
Do I have to notify the NAIH?	
Date of public notification	
Name of the notifying person	
Should stakeholders be informed?	
Date of information to stakeholders	
Date of entry (year, month, day)	

Serial number	
Scope of the personal data concerned	
Data subjects affected by the data breach	
Number of data subjects affected by a data breach	

[15] To be completed for each incident!
[16] For example: name, mother's name, address, e-mail address, etc.
[17] E.g. employee etc.

Date of the data breach	
Date of becoming aware of the data breach	
Nature of the data breach	
The circumstances of the data breach	
Impact of the data breach	
Measures taken to respond to the data breach	
Other data specified in the legislation providing for the processing	
Do I have to notify the NAIH?	
Date of public notification	
Name of the notifying person	
Should stakeholders be informed?	
Date of information to stakeholders	
Date of entry (year, month, day)	

Enacting provision:

These Rules shall enter into force on 30 August 2024.

Signed and approved by the CEO on 30 August 2024.

Issuing a document

Prepared by Dr. Fridman Robert Law Office

Dr. Fridman Róbert Ügyvédi Iroda
Dr. Fridman Róbert
ügyvéd
1054 Budapest, Bank u. 5. 1. em. 2.
Tel/Fax: 800-9094

He approved:

EWG Rail Zrt. 1.
1134 Budapest, Róbert Károly krt. 59.
Adószám: 26242387-2-41
Cégj.sz.: 01-10-049688

EWG Rail Ltd. represented by Gabor Miskolczi CEO