

PERSONAL DATA PROTECTION POLICY

Compliance Policies - Policy 7.5 - Data Protection

Originally approved by:	Board of Managers
Origin date:	August 24, 2014
Approved by:	Compliance Committee
Last revised date:	October 26, 2023
Policy owner:	Group Compliance Director
Contact:	Group Compliance Director

This document sets out ERG's Data Protection Policy with which the Group, Perimeters, Regions, Group Companies and their Employees must comply. The Perimeters, Regions and Group Companies may implement stricter rules where necessary to comply with local requirements.

In this document, unless otherwise stated, capitalized terms have the meaning ascribed to them in the section 3 (Definitions) below.

1. Policy Objective

- 1.1. Each Group Company, as part of running its business collects, stores and processes information about individuals. These can include Employees, contractors, suppliers, customers, Board of Managers members, directors, shareholders and guests. Group Companies respect the privacy of above-mentioned data subjects and their right to know what Group Companies are doing with their information.

Group Companies have a zero-tolerance approach to non-compliance with relevant legislation and regulation, including the 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 (General Data Protection Regulation, "GDPR") and (or) all local legislation applicable to Group Companies as amended from time to time.

This Policy facilitates business integration and consolidation by ensuring that privacy practices across Group Companies are consistent, aligned and designed to meet the business objectives. The nature of the Group's business, and the increasing need to integrate and operate globally requires privacy practices to be aligned globally.

- 1.2. The purpose of this Policy is to:
- 1.2.1. ensure that, with regard to Personal Data Processing, including its collection, storage and transfer, each Group Company conducts its business in compliance with all applicable laws and regulations, and that Personal Data is always protected and processed in accordance with the law applicable to it¹;
 - 1.2.2. define the types of Personal Data that Group Companies collect and the purposes for which we collect it;

¹ As at the date of publication of this Policy, this included, but not limited to:

In the **European Union**, the processing of personal data is governed by the General Data Protection Regulation 2016/679 ("GDPR").

In the **United Kingdom** it is the UK GDPR and the Data Protection Act 2018 (the Act).

In **Switzerland** it is the Federal Act on Data Protection of 19 June 1992

In **Kazakhstan** it is the Law of the Republic of Kazakhstan dated May 21, 2013 № 94-V "On Personal Data and its Protection"

In **Russia** it is the Law of the Russian Federation "On Personal Data" of 27.07.2006 No. 152-FZ with subordinate acts and other laws

In **South Africa** it is Act No. 4 of 2013: Protection of Personal Information Act, 2013 (POPI Act)

In **Brazil** it is the General Data Protection Law (LGPD), Federal Law no. 13,709/2018

In **China** – it is the Personal Information Protection Law (PIPL) dated August 20, 2021, and other laws;

In the **Kingdom of Saudi Arabia** – it is the Personal Data Protection Law, implemented by Royal Decree M/19 of 17.09.2021

- 1.2.3. outline each Employee's responsibilities for Processing that data in compliance with the applicable data protection laws and regulations; and
- 1.2.4. ensure that each Group Company operates standard Personal Data protection environment to allow transferring the Personal Data between Group Companies and ensure that Personal Data is adequately protected in line with applicable international data transfer laws when it is transferred across the borders.

2. Scope

- 2.1. This Policy applies to:
 - 2.1.1. all Group Companies and their Agents;
 - 2.1.2. all Employees; and
 - 2.1.3. all Personal Data collected, stored and otherwise processed by Group Companies during their business activities irrespective of the media it is carried on.
- 2.2. The Policy equally applies to all internal and external parties, including without limitation, individual contractors that (i) provide to the Group services affecting Personal Data and (ii) do not have an employment contract with the Group Company. Such contractors shall, for the purpose of this Policy only, be included in the definition of Employee.

3. Definitions

The below definitions are internal definitions, which while maintaining the meaning under applicable legislation, may have different names under local laws. While developing local policies and procedures, the Perimeters and Regions have the right to modify Policy provisions, taking into account the peculiarities of local laws, but should adhere to the terminology and principles of this Policy.

Agent – means a third party (natural person or a company) authorised to negotiate, represent or act on behalf of the Group Company on strategic matters, including but not limited to negotiating with government agencies, customs and clearing agents and lobbyists. It does not include bona fide professional advice or services rendered to the Group Company in the ordinary course of business where the Agent has no ability to bind the Group Company or negotiate or speak for the Group Company.

Board of Managers – means the Board of Managers of Eurasian Resources Group S.à r.l.

Company or ERG – means Eurasian Resources Group S. à r.l.

Compliance Committee – means the compliance committee of the Board of Managers.

Company Shareholders – means individuals and/or governmental or private entities owning shares in the Eurasian Resources Group S.à r.l. which entitle them to voting rights.

Customer Personal Data – means Personal Data collected in the process of regular customer relationship management, such as customer contact information, names and professional addresses.

Data Controller – means a natural or legal person, public authority, agency or any other body, which solely or jointly with others determines the purposes and means of Processing of Personal Data.

Data Protection Officer – means an individual assigned to advise and verify the Group's compliance with local data protection legislation and to serve as a contact point for internal and external requests from Data Subjects concerning collection and Processing of their Personal Data.

Data Processor – means a natural or legal person (including a Group Company), public authority, agency or any



other body that processes Personal Data on behalf of any of the Group Companies.

Data Protection Supervisory Authority – means an independent public authority that supervises, through investigate and corrective powers, the application of the applicable data protection laws.

Data Subject – means any identified or identifiable natural person to whom Personal Data relates.

Employees – means full-time, part-time and temporary personnel of any Group Companies, interns and contractors working within a Group Company's facilities or having access to Personal Data, including as part of access to Group Company's IT systems.

European Union ("EU") – means 27 Member States which form the European Union and which are subject to European legislation.

European Economic Area ("EEA") – means organization of countries including the EU members, Iceland, Lichtenstein and Norway, which have transposed certain legislation of the European Union into national law, and have agreed to fully comply with European legislation concerning Personal Data Protection.

General Data Protection Regulation ("GDPR") – means Regulation (EU) 2016/679 of the European Parliament and of the EU 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 Regulation 679/2018, the EU legislative act on privacy and data protection, meant to harmonizing the rules in this field. This regulation is applicable to all European Union and EEA countries governing the transfer and other processing of Personal Data of European and EEA Data Subjects whether such acts are performed inside or outside the European Union or EEA.

Group – means all Group Companies together.

Group Company – means ERG or its direct or indirect subsidiary in relation to which ERG exercises control (owns, directly or indirectly, more than fifty percent (50%) of the voting rights, or in which the power to control the entity is possessed by or on behalf of ERG).

Human Resources Personal Data – means Personal Data collected in the process of regular human resources administration, inter alia name, address, nationality, gender, marital status, social security number and bank account.

Joint Controller – means two or more Data Controllers jointly determining the purposes and means of the same Processing.

Outside Representative – means a non-Group Company person assigned by Compliance Department to represent the Group Company offices without a Data Protection Officer. The Outside Representative serves as a contact point for Personal Data related questions from EU and EEA citizens and residents located permanently or temporarily outside EU or EEA countries.

Perimeter – means an aggregate of several Regions and/or countries, in which the Group operates, including the International Perimeter and the Kazakhstan Perimeter.

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, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Even if it is not immediately obvious whether a person can be identified, a person may still be identifiable if the Group Companies have or may have reasonable means available to it to be able to identify that person.

Personal Data Breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Policy – means the present document titled "Personal Data Protection Policy".

Processing – means any operation or set of operations performed upon Personal Data, whether or not by

automated or electronic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Regions – means the regions in which the Group operates, including Africa, Brazil, Kazakhstan region and other regions.

Sensitive (Special Category of) Personal Data – means Personal Data as defined by the General Data Protection Regulation and other non-EU local laws which reveals a Data Subject's physical or mental health, religious or similar beliefs, political opinions, racial or ethnic origin, trade union membership, or criminal offences, criminal background, sexual orientation, sex life as well as genetic data or other Personal Data, which local regulations define as Special Category of Personal Data.

Shareholder Personal Data – means the Personal Data belonging to the following Data Subjects:

- ultimate beneficiaries of the Group or individuals designated as such;
- members of the Board of Managers;
- directors, employees and other representatives or Agents of the direct and indirect shareholders of the Company;
- any other managers and executives of the Group Companies unless they are employees of the Group.

Sub-processor – means a third-party individual or legal person, company who is engaged by the Data Processor and has or potentially will have access to or process Personal Data.

Supplier Personal Data – means Personal Data collected in the process of supplier relationship management, such as supplier contact information, name and professional address.

4. Policy Statements

- 4.1. Each Group Company processes Personal Data in compliance with applicable data protection laws and regulations.
- 4.2. Each Group Company and all business units, irrespective of jurisdiction, shall follow the following minimum standards of practice:
 - 4.2.1. Fair and lawful Processing of Personal Data: Group Companies process Personal Data in a fair and lawful manner, which requires, among others, the following:
 - a) Lawful use: Personal Data may not be used in ways that have unjustified or disproportional adverse effects on a Data Subject and/or could be unlawful;
 - b) Transparency: Group Companies must be transparent with Data Subjects about their Processing activities (in particular on the existence and conditions of Processing);
 - c) Purpose limitation: Personal Data must be obtained only for specified and lawful purposes and used only in ways a Data Subject would reasonably expect it to be used. It must also only be Processed in a manner compatible with the purposes for which it was collected;
 - d) Adequacy/Data minimisation: Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
 - e) Accuracy: Personal Data must be accurate and kept up to date;
 - f) Storage limitation: whilst Personal Data must be kept in accordance with relevant Group policies and applicable laws, it must not be kept in a form which identifies the Data Subject for longer than is necessary for the purpose for which it is being processed. By way of principle, Personal Data should be destroyed, deleted or anonymised once the purpose for which they

are processed no longer exists;

- g) Integrity and confidentiality: Processing Personal Data in a manner that ensures appropriate security of Personal Data, including protection against unauthorised or unlawful Processing, accidental loss, destruction or damage, using appropriate technical and organisational measures;
 - h) Accountability: Group as Data Controller shall be responsible for and be able to demonstrate compliance with the GDPR and other applicable privacy laws and regulations;
 - i) Respect for the rights of Data Subjects: each Group Company must respect and give effect to the statutory rights of Data Subjects where it processes their Personal Data.
- 4.2.2. Prior information and/or consent: if required by local law, a Group Company should give Data Subjects the required information (e.g. privacy notices) about the Personal Data it is collecting and how it will be processed² and, if required by local law, obtain specific, explicit, informed, freely given and unambiguous consent to that effect from the Data Subject.

Consent may not be indicated by the Data Subject's inaction or by use of a pre-checked box. Privacy notices should be made available to Data Subjects (e.g. published on all of the Group Companies' internet websites and published on other communication tools) and should be reviewed and updated due to legislation changes or in case of necessity (i.e. change in purpose of the Processing, new type of Personal Data is processed or any other content change).

- 4.2.3. Data security: each Group Company is required to take appropriate technical, physical and organisational measures including protection against unauthorised or unlawful Processing of Personal Data and against accidental loss, destruction or damage:
- a) Information security is managed through the Information Security policies and procedures. The information security functions should be timely informed by the data owner to ensure effective controls will be implemented to ensure the data security of Processing;
 - b) Each Group Company is also responsible for all Processing carried out by Data Processors or Joint Controllers on that Group Company's behalf. Group Companies take relevant measures, including, where applicable, through conducting a detailed due diligence on potential Data Processors or Joint Controllers and inclusion of special data protection terms and conditions in contracts with them as required by data protection law and regulations, including Article 28 of the GDPR;
 - c) Employees that want to engage a Data Processor to carry out processing on a Group Company's behalf must conduct a detailed due diligence of data Processing standards by the Data Processor and contact the relevant Data Protection Officer of the Perimeter or Region and, if necessary, the respective Legal Department to ensure that suitable contractual data protection terms and/or additional privacy agreements and/or clauses are put in place and to ensure, via the performance of risk analyses, audits, privacy impact assessments and reviews that data protection laws and regulations are complied with by each Data Processor.

4.3. Each Perimeter or Region and, where the applicable law requires, each Group Company should designate a responsible Employee or an Outside Representative to act as their Data Protection Officer, who shall:

- 4.3.1. be responsible for local implementation and ensuring compliance with the Policy and applicable Personal Data protection laws and regulations;

² Depending on applicable local data protection rules, each Group Company may need to inform Data Subjects on (i) its identity or corporate name; (ii) in certain cases, what type of personal data are collected or processed; (iii) for which purposes personal data is processed; (iv) whether personal data will be shared with anyone else, even transferred outside of the place of collection; and (v) their statutory rights and how they can exercise them.

- 4.3.2. be responsible for establishing processes, procedures and registers to ensure compliance with the Policy and applicable Personal Data protection laws and regulations;
 - 4.3.3. be the responsible and single point of contact for liaising with local Data Protection Supervisory Authorities;
 - 4.3.4. determine, together with the Heads of Group Companies involved in the Processing, the purposes for which and the manner in which any Personal Data is processed by each Group Company, and if such purposes and manners are compliant with local laws;
 - 4.3.5. handle Group Companies' and Employees' questions and concerns about the implementation of and compliance with Policy and applicable Personal Data protection laws and regulations;
 - 4.3.6. receive questions, requests and complaints from Data Subjects regarding data protection or data security issues, and act as the primary contact point for Data Subjects' requests tending to the exercise of their statutory rights.
- 4.4. In the absence of a delegation at the Perimeter or Region level, the senior regional Compliance Officer of the Perimeter or Region or their delegate shall be deemed to be, and fulfil the function of, the Data Protection Officer.
- 4.5. The Heads of Group Companies, with assistance of their Data Protection Officer, must implement appropriate Personal Data protection measures that are as protective as, or more protective, than those defined in this Policy, and which ensure compliance of its Employees with the Policy and the applicable local laws relating to Personal Data protection.
- 4.6. Employees must report any Personal Data Breach, whether confirmed or suspected, to the Data Protection Officer immediately. Failure to do so will result in disciplinary measures up to and including termination of employment or contracting relationship.
- 4.7. Employees shall follow the Group and Perimeter Personal Data Breach Procedures in case of any data-related incidents, which includes informing all relevant and responsible personnel, governance bodies, regulators, etc.
- 4.8. The Data Protection Officer will independently make the final decision on informing the local Data Protection Supervisory Authority of Personal Data Breaches within 72 (seventy-two) hours after its discovery according to Personal Data Breach Procedure and applicable laws and regulations.
- 4.9. The Data Protection Officer shall keep a record of all Personal Data Breaches, including actions taken to mitigate risks by the Group Company, contacts with local Data Protection Supervisory Authorities, and the justification if a Personal Data Breach was not reported to the relevant Data Protection Supervisory Authority and the possibly affected Data Subjects.
- 4.10. Each Group Company acting as Data Controller, Joint Controller or Data Processor will inform the Data Protection Officer of all Personal Data Processing operations as required under applicable laws. Where necessary, the Data Protection Officer will delegate Employees to carry out data protection impact assessments where they determine that a particular Processing, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of Data Subjects.

5. Rules

Purposes for Processing:

- 5.1. Group Companies may process Personal Data for the following purposes only:

Human Resources Personal Data

5.1.1. Human Resources Personal Data encompasses the following types of Personal Data:

- a) Personal identification information such as name, home address, date of birth, gender, work-related photographs, personal email address, personal mobile (and home, if applicable) phone number;
- b) Government-issued identification numbers, such as national ID or unique in-company identifier used for payroll purposes and management of access to information systems;
- c) Employment permissions, such as immigration, right-to-work and residence status and related documents;
- d) Financial information, such as payroll and payment or benefits related information, including salary and insurance information, tax numbers, tax cards, bank account details, tax related invoices, and employment related benefits information, including information on beneficiaries;
- e) Emergency contact details and limited amount of family or beneficiary information including contact data of family members for emergency cases, Personal Data of Employees' family members required to apply for residence permits (e.g. citizen service number, full name, gender, date of birth, place of birth, nationality, civil status), Personal Data of family members requested by insurance companies for the conclusion of insurance contracts as well as Personal Data of beneficiaries and dependents for the pension plan arrangement (e.g. full name, date of birth, place of birth, relation to Employee);
- f) Job-related information, such as years of service, work location, employment ID, work email address, work record, vacation, sick leave and other leave absences, business trip information, business trip related invoices and contract data;
- g) Educational and training information, including any certifications obtained prior to or during employment, as well as recruitment and performance-related data, such as objectives, ratings, comments, feedback results, career history, work equipment, career and succession planning, skills and competences and other work-related qualifications;
- h) Compliance and risk management information, such as disciplinary records, background check reports and security data;
- i) Office attendance information at an ad hoc basis and only when the circumstances would justify it (e.g. suspected fraudulent activities), the presence of the Employee at the office, including the date and time of the entry into and exit out of the office;
- j) Group IT usage information, Group's IT and information assets (including company laptops and desktops) are monitored in accordance with applicable laws. Such monitoring includes, on a general basis, login/logout date and time at device and application level. In justified cases, such as information security compliance monitoring or alleged misconduct (e.g. violations of Group policies or instructions) and unlawful behaviour (e.g. fraud, theft or abuse), monitoring may include online traffic data, email traffic data and website visits, and monitoring of document usage (including frequency, size, format, opening, modification and sharing of documents).

5.1.2. Human Resources personnel may process Human Resources Personal Data in the course of conclusion, performance or termination of employment contracts / taking of pre- and post-contractual measures, as well as in order to comply with the respective Employee privacy notice and the Group Companies' legal obligations or to pursue their legitimate interests to the extent permitted by local labor law with regard to:

- a) managing (local and cross-national) staff and teams of Employees across different jurisdictions; allowing intra-group job rotation;

- b) administrative management of Employees, including performance of employment contracts, compliance with applicable social, tax and labour laws and regulations;
 - c) managing general human resources administration including recruiting, hiring, payroll, leave, training, evaluations, head count analysis, career and senior staff succession planning.
- 5.1.3. The manager of an Employee, and general management, on a need-to-know basis, may also process Human Resources Personal Data for that particular Employee to perform obligations under employment contracts or to comply with a Group Company's legal obligation or to pursue its legitimate interests with regard to managing (local and cross-national) staff and teams of Employees across different jurisdictions; and managing, recruiting, hiring, staff evaluations and senior staff succession planning.
- 5.1.4. Accounting personnel may process Human Resources Personal Data to comply with Group Companies' legal obligations with regard to managing accounts, payroll, benefits and taxes and other deductions, contributions and allowances.
- 5.1.5. The remuneration committee of the Board of Managers or similar, if any, may process Human Resources Personal Data to perform obligations under employment contracts or to comply with a Group Company's legal obligation to determine Employee's remuneration.
- 5.1.6. Other departments' Employees may process Human Resources Personal Data only to the extent necessary and sufficient to perform their functions, including as part of physical security, occupational health and safety, healthcare, investigations and inspections, and other similar functions.

Personal Data of Employees Leaving a Group Company

When an Employee leaves a Group Company, the latter shall do the following:

- 5.1.7. give each departing Employee, in case stipulated by the applicable legislation, the opportunity to make copies and/or the possibility to destroy of his/her private files and folders stored in his/her business e-mail in-boxes and corporate computers and mobile computing devices before his/her leaving;
- 5.1.8. deactivate the Employee's corporate e-mail address as soon as reasonably possible after the Employee's departure.

Training Programme

- 5.1.9. All Employees who have permanent and/or regular access to Personal Data will complete training on the collection and Processing of Personal Data or in the development of tools used to process Personal Data on a periodic basis.
- 5.1.10. All other Employees will receive training on this Policy upon joining the Group and as needed thereafter.

Customer Personal Data

- 5.1.11. Employees may process Customer Personal Data only in support of customer relationship management to perform a Group Company's contractual obligations, ensuring commonality of approach towards customers, and managing a Group Company's customer contracts (CRM), to comply with a Group Company's legal obligation or to pursue its legitimate interests.

Supplier Personal Data

- 5.1.12. Employees may process Supplier Personal Data only in support of supplier management to perform a Group Company's contractual obligations, to comply with a Group Company's legal obligations or

to pursue its legitimate interests with regard to fulfilling its resource requirements, ensuring commonality of approach towards suppliers and managing a Group Company's supplier contracts.

Shareholder Personal Data

5.1.13. Processing of the Shareholder Personal Data shall be based on:

- consent;
- applicable legal requirements;
- legitimate interest of the Group.

5.1.14. The Corporate secretary of ERG is responsible for obtaining valid consents from the Company Shareholders for processing of Shareholder Personal Data.

5.1.15. In order to comply with the requirements of the law, as well as within the framework of ensuring the legitimate interests of the Group, it is possible to disclose the Shareholder Personal Data under Know Your Customer (KYC) and Anti-money Laundering (AML) procedures, as well as public disclosure within the limits established by applicable legislation.

5.1.16. Shareholder Personal Data shall be kept by the designated Employees in a secure location which is only accessible by them, with the necessary support of IT.

5.1.17. The renewal of the Shareholder Personal Data, verification of their accuracy and relevance shall be carried out at least once every 6 (six) months.

5.1.18. Any requests concerning Shareholder Personal Data or any other KYC/AML requests shall be sent to the Head of Corporate & Finance Support as designated by the Group Chief Legal Officer. Head of Corporate & Finance Support together with the Data Protection Officer of the Perimeter or Region are responsible for verifying that the requested Shareholder Personal Data will be processed in accordance with this Policy and the applicable laws.

5.1.19. The Corporate secretary of ERG shall notify the Company Shareholders about the use of their Personal Data every 6 (six) months.

Sensitive Personal Data (Special Categories of Personal Data)

5.1.20. The Processing of Sensitive (Special Categories of) Personal Data must be carried out in strict accordance with the requirements of applicable legislation. Prior to Processing Sensitive Personal Data, review by the Data Protection Officer of the Perimeter or Region is required to determine, if such Processing will impact the rights and freedoms of the Data Subject.

5.1.21. Only the following Sensitive (Special Categories of) Personal Data can be processed by Group Companies:

- a) religious affiliation for withholding tax purposes³;
- b) medical records⁴;
- c) biometric data;
- d) trade union membership.

5.1.22. Sensitive Personal Data should only be accessible to Employees as permitted by local labor and data protection legislation and on a strict need-to-know basis. Sensitive Personal Data shall only be

³ E.g. in Switzerland

⁴ Applicable to those business units which provide Company-employed medical services or which conduct or collect results of medical tests (e.g. alcohol or drug testing, etc.), provide and (or) support relevant IT systems or pay for medical services.

accessible to Group Companies that are obliged and (or) have the right to process such data under applicable local legislation.

IT-related Personal Data

- 5.1.23. Each Group Company may process Personal Data in relation to the use of the day-to-day IT system which enables Employees and external parties to, inter alia, exchange emails, access internet website, store files/data, use software applications and generate, maintain and store IT traces and log files as required or permitted under applicable laws.
- 5.1.24. If local laws and regulations require an authorisation (e.g., by a data protection or other local authority) for the Processing of Sensitive (Special Categories of) Personal Data (e.g. for Employees IT-monitoring), then the Group Companies shall obtain such authorisation in a timely manner and shall inform the concerned Data Subjects.
- 5.1.25. In Processing IT related Personal Data, Group Companies shall follow the applicable privacy rules, such as the secrecy of correspondence or private electronic communications.

Other Personal Data

- 5.1.26. Employees may also process Personal Data as described in the policies and procedures on information security and policies and procedures concerning the acceptable use of information assets. The purpose and scope of such processing is further described in those policies.

Transparency, Information and Data Subjects' rights

- 5.2. Most Personal Data received by Group Companies is provided directly by the Data Subject. When collecting Personal Data, each Data Subject, if required by local law, must be informed of the following⁵:
 - 5.2.1. the corporate name of the Group Company (or Group Companies) collecting the information as the Data Controller;
 - 5.2.2. the name and contacts of Data Protection Officers of the Perimeter or Region, or Outside Representative that the Data Subject may contact regarding his/her Personal Data;
 - 5.2.3. the purpose(s) of such Processing as well as the legal basis for the Processing;
 - 5.2.4. the legitimate interests pursued, where applicable;
 - 5.2.5. the Group or third-party recipients (referred to either individually or collectively through generic names such as 'Group Companies or 'local authorities') who will receive the Personal Data in order to process it for their own independent purposes (for the sake of clarity, identity of Data Processors and Sub-processors do not need to be disclosed to Data Subjects);
 - 5.2.6. if the Data Controller is an EU entity and where applicable, that the Data Controller intends to transfer Personal Data to a recipient based outside of the European Union/EEA and:
 - whether the third country in question provides an adequate level of protection to Personal Data according to EU standards (that is, whether an adequacy decision by the European Commission exists or not) and, in the negative,
 - a reference to the appropriate or suitable safeguards adopted by the Data Controller to secure the transfer, the means to obtain a copy of them or where they have been made available; and
 - the name and contact of the Data Protection Officer of the Perimeter or Region, or Outside Representative that the Data Subjects may contact regarding their Personal Data.

⁵ Such information may be part of a contract, job application template or Employee Privacy Notice.

- 5.2.7. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- 5.2.8. if the Data Controller is an EU entity, the Data Subject's statutory rights, in the European Union for instance, include:
- the right to request access to and rectification or erasure ("to be forgotten") of Personal Data (subject to conditions);
 - the right to ask for the restriction of Processing concerning the Data Subject (subject to conditions);
 - the right to object to the Processing (subject to conditions). Data Subjects have right to object at any time on compelling legitimate grounds relating to his/her particular situation to the Processing of his/her Personal Data, unless such Processing is required by law. They have a right to object, free of charge, to the Processing of Personal Data for the purpose of direct marketing;
 - the right to Personal Data portability; as well as
 - the right to lodge a complaint with the competent Data Protection Supervisory Authority.
- 5.2.9. When Personal Data is obtained from a third party, Group Companies should, within reasonable period after obtaining Personal Data, but at the latest within one month, having regard to the specific circumstances in which Personal Data is Processed, inform the Data Subject of the categories of Personal Data concerned, the source from which his/her Personal Data originates and if applicable, whether it came from publicly accessible sources. Please see the respective Group Data Subject Rights Handling Procedure.
- However, the obligation to inform the Data Subject in such a case may not apply if the Data Subject already has the relevant information.
- 5.2.10. Requests from Data Subjects concerning their rights should be addressed to Data Protection Officer of the Perimeter or Region. Response to Data Subjects must be provided within one month. However, if the request is complex or the Group Companies receive large number of requests this term may be extended by a further two months. In the latter case, the Data Protection Officer of the Perimeter or Region shall provide an appropriate explanation to the Data Subject about the reason of the extension.

Automated Decisions⁶

- 5.3. No evaluation of, or decision about, any Data Subject which significantly affects him/her will be based solely on automated/electronic Processing of Personal Data unless that decision is:
- 5.3.1. taken in the course of entering into or performing a contract, provided the request lodged by the Data Subject has been satisfied or there are suitable measures to safeguard the Data Subject's legitimate interests, such as arrangements allowing the Data Subject to put forward his or her point of view; or
- 5.3.2. authorised by law which also specifies measures to safeguard a Data Subject's legitimate interests.

Data Subjects have the right to be notified, if a Group Company has made a decision about him/her that is based on automated data Processing alone, so that (s)he can request human intervention in any automated Processing.

Data Retention

⁶ Examples of automated decisions include automated review of initial contract bids or automated review of employment candidate questionnaires.

- 5.4. Group Companies shall retain Personal Data, both electronic and hardcopy, in accordance with the relevant Group Company's policies, and as applicable, the established retention schedule, which must comply with applicable legislation and be updated in a timely manner.

Security and Confidentiality

- 5.5. Appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access should be implemented and maintained by each Group Company as per the Information Security policies and procedures requirements.
- 5.6. In the event of an accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access to Personal Data, Group Companies will follow the procedures established under the applicable data protection laws, Group Company policies and procedures (i.e. Group Personal Data Breach Procedure) and the instructions of the competent Data Protection Supervisory Authorities. In the case of an EU Group Company which acts as a Data Processor:
- it shall inform the Data Controller of any Personal Data Breach without undue delay after becoming aware of the event; and
 - if in the opinion of the Data Protection Officer notification is necessary, the Data Protection Officer shall notify any Personal Data Breach to the competent local Data Protection Supervisory Authority without undue delay and where feasible not later than 72 hours after its awareness. Such notification shall include all information required under applicable data protection laws. In addition, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subject, the Data Controller shall communicate the Personal Data Breach to the concerned Data Subjects without undue delay, save if it can be documented that a statutory exemption applies.

Sharing of Personal Data within Group Companies

- 5.7. ERG is a global company and will occasionally need to share Personal Data with Group Companies.
- 5.8. Personal Data will only be disclosed to other Group Companies in accordance with this Policy and applicable laws. Personal Data is protected when processed by any Group Companies through adherence to the common strict organisational and technical safeguards as set out in the respective (privacy) laws and regulations on confidentiality, information security and other applicable policies and procedures and this Policy.
- 5.9. Intra-group agreements - which include standard contractual clauses and Personal Data Processing agreements - should be used to allow possible transfer of Personal Data between Group Companies.

Sharing of Personal Data with Data Processors, Data Controllers and Joint Controllers

Sharing of Personal Data by Group Companies located in the EU with Data Processors, Data Controllers and/or Joint-Controllers located within the EU or assimilated countries

- 5.10. If a Group Company based in the EU wishes to share Personal Data with a Data Processor, Data Controller or Joint Controller that is based in the EU, the EEA or in a country recognised by the European Commission as ensuring an adequate level of protection⁷, the following must occur prior to transferring the Personal Data:
- 5.10.1. there must be a written contract between the Group Company and the Data Processor/ Data Controller/Joint Controller; and

⁷ The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and LED and Uruguay (See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en for current information).

- 5.10.2. such contract should be based on, or contain equivalent provisions to, the Personal Data Processing agreement template validated by the Group and available from the Data Protection Officer – Europe.

Sharing of Personal Data by Group Companies located in EU with Data Processors, Data Controllers or Joint-Controllers located outside the EU or assimilated countries

- 5.11. If a Group Company based in EU wishes to share Personal Data with a Data Processor, Data Controller or Joint Controller located outside the EU, the EEA or in a country that is not recognised by the European Commission as ensuring an adequate level of protection, the responsible Employee must ensure the following:
- 5.11.1. that the transfer occurs subject to a binding intra-group agreement (if the Data Processor/Joint Controller is one of the Group Companies);
 - 5.11.2. perform a data protection impact assessment;
 - 5.11.3. if no such intra-group agreement is in place, the Group Companies must enter into a written contract based on, or containing equivalent provisions to, the Personal Data Processing agreement template validated by and available from EU Legal;
 - 5.11.4. all transfers of Personal Data must be secure and in compliance with applicable law relating to international data transfers;
 - 5.11.5. the relevant Group Company exporting the Personal Data must have (i) entered into an appropriate set of standard contractual clauses in a form approved by the European Commission with the Data Processor/Data Controller or Joint Controller prior to the Personal Data being transferred; and (ii) carry out potential formalities or filings required by its local legislation.

Sharing of Personal Data by Group Companies located outside EU

- 5.12. If a Group Company based outside EU wants to share Personal Data with a Data Processor, Data Controller and/or Joint Controller located outside their home country the Data Protection Officer of the Perimeter or Region should make sure that the transfer is conducted in full compliance with local laws and regulations governing data protection and international transfers of Personal Data.

6. Handling questions, concerns and enquiries

- 6.1. If an Employee has any questions or concerns in relation to Personal Data protection, he/she should contact his/her Data Protection Officer of the Perimeter or Region.
- 6.2. If any Data Subject believes that his/her Personal Data is not processed in compliance with this Policy he/she should raise his/her concern to the respective Data Protection Officer.
- 6.3. If an Employee receives a complaint from a Data Subject outside of the Group, such complaint must be forwarded without undue delay to the respective Data Protection Officer.
- 6.4. The Data Protection Officer will review the complaint on a confidential basis. In the event of absence of the Data Protection Officer, the Chief Legal Officer of the Perimeter or Region will review and forward to the Data Protection Officer as soon as (s)he is available.
- 6.5. The respective Group Company, with notice to the Data Protection Officer of the Perimeter or Region, will initiate an investigation into any allegation of violation of this Policy.
- 6.6. Employees are required to cooperate with internal investigations related to possible Policy violations.
- 6.7. In order to allow the Group to properly investigate a concern, allegations of non-compliance with or violation of this Policy should include sufficient information concerning the incident or the violation.

- 6.8. The Group will treat the identity of any individual making a complaint as confidential. However, in certain circumstances, the Group may be obliged by law to disclose the information or the identity of the person submitting the complaint or allegation to the respective authorities.
- 6.9. Each complaint and any information relating to a complaint will be retained in written and/or electronic form by the respective Data Protection Officer until the complaint has been resolved, or as required by law and otherwise in accordance with the Group Company policies and applicable laws and regulations.

7. Responsibilities

- 7.1. The Compliance Committee is responsible for establishing this Policy.
- 7.2. The Compliance Department of the respective Perimeter or Region is responsible for:
 - 7.2.1. Providing guidance and advice to the Perimeters CEOs or Heads of Regions with regard to the implementation of this Policy and oversight of the implementation of this Policy;
 - 7.2.2. Monitoring of compliance with this Policy;
 - 7.2.3. Reporting requirement: preparation of periodical reports on the status of implementation and adherence to the Policy.
- 7.3. The Perimeters CEOs and Heads of Regions are responsible for effective implementation of this Policy in their respective areas of responsibility and make sure that adequate controls are implemented to ensure on-going compliance.
- 7.4. The Perimeters CEOs and/or Heads of Regions are responsible for designating a Data Protection Officer (if applicable) and approval and enforcement of respective Perimeter's or Region's policies and procedures developed by the Data Protection Officer.
- 7.5. Data Protection Officers are responsible for establishing appropriate responsibilities, procedures, training and internal controls within their respective Perimeter or Regions to ensure the consistent implementation of this Policy and compliance with its requirements.
- 7.6. It is the responsibility of the Perimeters CEOs and Heads of Regions to ensure that their respective Employees and Data Processors/Data Controllers/Joint Controllers used are made aware of this Policy requirements and that Employees processing or having access to Personal Data are periodically trained in data protection requirements.

8. Monitoring and Audit

- 8.1. The Data Protection Officer of the Perimeter or Region should, on an annual basis or on demand, report on the status of compliance with this Policy to the Compliance Committee.
- 8.2. The Group shall arrange for periodical independent review of compliance with this Policy and report any deficiencies and respective recommendations to the Group management and the Compliance Committee.

9. Non-compliance

- 9.1. Any non-compliance with the Policy should be documented and reported to the Data Protection Officer, Compliance Department or the ERG Hotline.
- 9.2. It is the responsibility of each Employee to comply with the terms of this Policy. Employees who violate this Policy will be subject to disciplinary measures subject to local law, up to and including termination of their employment.

10. Revision Process

- 10.1. This Policy shall be reviewed periodically (but not less than once every 2 years) and updated where needed to reflect any changes in the relevant law and/or business requirements.
- 10.2. All requests for amendments to this Policy shall be directed to the Policy owner or the Data Protection Officer.
- 10.3. Amendments to this Policy must be made in accordance with the internal documents of the Company.

11. Document Version Control

Version	Approved by	Date of approval	Comments
1.0	Board of Managers	24.08.2014	
1.0	Compliance	05.05.2015	
2.0	Board of Managers	13.03.2016	
3.0	Board of Managers	27.08.2017	
4.0	Board of Managers	02.06.2018	
5.0	Compliance Committee	26.10.2023	