DATA PROTECTION POLICY

Compliance Policies - Policy 7.4 - Data Protection

Approved by	The Board of Managers
Origin Date:	August 24, 2014
Last Revised Date:	June 2, 2018
Policy owner(s):	Group Head of Compliance
Contact(s):	Head of Compliance International

In this document, the "Company" or "ERG" means Eurasian Resources Group S.a.r.l. and includes, where applicable, all direct and indirect subsidiaries.

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 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 and Group Companies have a zero tolerance approach to non-compliance with relevant legislation and regulation, including but not limited to 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).

1.2. The purpose of this Policy is to:

1.2.1. ensure that, with regard to personal data collection, storage, processing 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 it[1];

1.2.2. define the types of Personal Data that Group Companies collect and the purposes for which we collect it;

1.2.3. outline each Employee's responsibilities for collecting and 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.

[1] *For example, in the **European Union**, the processing of personal data is governed by the General Data Protection Regulation 679/2016 ("GDPR") and other implementing texts. In the **United Kingdom** it is primarily the GDPR and the Data Protection Act 2018 (the Act), but also other regulations.*

*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 (e.g. code on administrative infractions)*
*In **South Africa** it is Act No. 4 of 2013: Protection of Personal Information Act, 2013*
*In **Brazil** there is currently no general data protection law. Nevertheless, a number of specific laws including Internet Rights Bill (Marco Civil da Internet) and specifying the consumer protection code (Codigo de Defensa de Consumidor) address various privacy and data protection issues. There is however a draft data protection bill under discussion in the Brazilian Congress.*
*In **China –** Decision on Strengthening the Protection of Network Information 28 December 2012; Regulation on Employment Service and Employment Management; Measures for the Punishment of Conduct Infringing the Rights and Interests of Consumers*
*In **United Arab Emirates** – There is no general federal data protection law in the United Arab Emirates (UAE) comparable to those applicable in Europe although organizations which belong to the International Financial Center of Dubai (DIFC) are governed by comprehensive general data protection laws.*

2. Scope

2.1. This policy applies to:

2.1.1. all Group Companies (as defined below) and their agents;

2.1.2. all Employees; and

2.1.3. all Personal Data collected, stored and processed by Group Companies during their business activities irrespective of the media it is carried on.

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 procedures Regions should follow the terminology and legal concepts used in their respective country laws, while ensuring compliance with the Policy principles.

3.1. **The Board** – the Board of Managers of Eurasian Resources Group SARL.

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

3.3. **Data Controller** - 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 Personal Data.

3.4. **Data Protection Officer** – 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.

3.5. **Data Processor** - 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.

3.6. **Data Subject** - any identified or identifiable natural person to whom Personal Data relates.

3.7. **Employees** - full-time, part-time and temporary personnel of any Group Companies, interns and contractors working within a Group Company's' facilities or accessing a Group Company's IT systems.

3.8. **European Union** - The 28 Member States which form the European Union and which are subject to European Legislation.

3.9. **European Economic Area ("EEA")** - European countries which have transposed certain legislation of European Union into national law, and have agreed to fully comply with European legislation concerning Data Protection.

3.10. **Human Resources Personal Data** - Personal Data collected in the process of regular human resources administration, such as name, address, nationality, gender, marital status, social security number and bank account.

3.11. **General Data Protection Regulation** - 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 Regulation 679/2018, the EU legislatory act on privacy and data protection, meant to harmonizing the rules in this field. This regulation applicable to all European Union and EEA countries governing the transfer and processing of Personal Data of European and EEA Data Subjects whether such acts are performed inside or outside the European Union or EEA.

3.12. **Group Companies** - includes Eurasian Resources Group SARL and any entity in which it 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 Eurasian Resources Group SARL.

3.13. **Group Company Shareholders** – Individuals, and/or governmental or private entities owning shares in the Group Companies which entitle them to voting rights.

3.14. **Outside Representative** – A non-Group Company person assigned by Compliance 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.

3.15. **Personal Data** - any information of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person. A natural person will be considered to be identifiable if he/she 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 one or more factors specific to his/her physical, physiological, genetic, mental, cultural, social or economic, identity. 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.

3.16. **Personal Data Breach** – 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.

3.17. **Processing** - 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.

3.18. **Regions** - a group of one or more Group Companies located in the same geographical area. Group regions are Kazakhstan, Africa, Brazil and Europe.

3.19. **Sensitive Personal Data** – Personal Data as defined by the European Commission' 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, sexual orientation, sex life as well as genetic data.

3.20. **Supplier Personal Data** - Personal Data collected in the process of regular supplier relationship management, such as supplier contact information, name and professional address.

4. Policy Statements

4.1. Each of the Group Companies 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) Retention: 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 or anonymised once the purpose for which they are processed no longer exists.

g) Respect for the rights of Data Subjects: each of the Group Companies 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 basic information about the Personal Data it is collecting and how it will be processed[2] and, if necessary by local law, obtain clear and explicit 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).

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.

b) Each Group Company is also responsible for all Processing carried out by Data Processors on that Group Company's' behalf. Group Companies fulfil this responsibility through conducting a detailed due diligence on potential Data Processors and inclusion of special data protection terms and conditions in contracts with them as required by data protection law and regulations, especially by article 28 of the General Data Protection Regulation.

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 local general counsel and the relevant regional Data Protection Contact to ensure that suitable contractual data protection terms are put in place and to ensure, via the performance of risk analyses, audits and reviews that data protection laws and regulations are complied with by each Data Processor.

4.3. Each Region should designate a senior officer to act as their Data Protection Contact, who shall:

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

4.3.2. be responsible for establishing procedures to ensure compliance with the Policy and applicable data protection laws and regulations;

[2] *For example, depending on applicable local data protection rules, each Group Member may need to inform Data Subjects on (i) its identity or corporate name; (ii) in certain cases, what data are collected or processed; (iii) for which purposes data is processed; (iv) whether data will be shared with anyone else; and (v) their statutory rights and how they can exercise them.*

4.3.3. be responsible for liaising with local Data Protection Authorities;

4.3.4. determine, together with the business unit heads 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 data protection laws and regulations;

4.3.6. receive questions or complaints by Data Subjects regarding data protection or data security issues, and act as primary contact point for Data Subjects' requests tending to the exercise of their statutory rights.

4.4. In the absence of a regional delegation, the senior regional Compliance Officer or their delegate shall be deemed to be, and fulfil the function of, the Data Protection Contacts.

4.5. The business unit heads, with assistance of their Data Protection Contacts, must implement appropriate 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 data protection.

4.6. Employees must report any 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 relations.

4.7. The Data Protection Officer shall immediately inform the local general counsel or Chief Legal Officer, the Group Head of Compliance, the Group Head of Risk and Head of Information Security of any data protection risks, potential compliance issues and Personal Data Breaches.

4.8. The Data Protection Officer will, independent of the opinions of the local general counsel or Chief Legal Officer, the Group Head of Compliance, the Group Head of Risk and Head of Information Security, and members of the Board or other Group Company officers, have the final decision on informing the local Data Protection Authority of Personal Data Breaches within 72 hours after its discovery according to Policy Procedures.

4.9. The Data Protection Officer shall keep a record of all Personal Data Breaches, including actions taken to limit risks by the Group Company, contact with local Data Protection Authorities, and the justification if a Personal Data Breach was not reported to the applicable national Data Protection Authority.

4.10. Each EU Group Company acting as Data 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 Personal Data:

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

Human Resources Personal Data

5.1.1. Human Resources personnel may process Human Resources Personal Data to perform employment contracts/take pre-contractual measures, to comply with 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 staff 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;

d) Personal identification information, such as name, home address, date of birth, gender, work- related photographs, and home phone number; Personal identification information, such as name, home address, date of birth, gender, work- related photographs, and home phone number;

e) Government-issued identification numbers, such as national ID for payroll purposes and management of access to information systems;

f) Immigration, right-to-work and residence status;

g) Emergency contact details and limited amount of family information;

h) Job-related information, such as years of service, work location, employment ID, work record, vacation absences, and contract data;

i) Educational and training information 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;

j) Information related to the usage of ERG's IT assets;

k) Information needed for compliance and risk management, such as disciplinary records, background check reports and security data; and

l) Payroll and payment or benefits-related information, such as salary and insurance information, tax numbers, bank account details, and employment related benefits information

5.1.2. 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 staff across different jurisdictions; and managing, recruiting, hiring, staff evaluations and senior staff succession planning.

5.1.3. 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.

5.1.4. The Remuneration Committee 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 remuneration.

Customer Personal Data

5.1.5. 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

5.1.6. 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

5.1.7. The Company Secretaries for each of the Group Companies and nominated employees of Legal Services (as designated by the Chief Legal Officer) may process, store and use the Personal Data of the shareholders, their directors, the Board, beneficiaries of the Group, officers and senior management of the Group Companies only if it is necessary for the concerned Group Company in order to comply with applicable law, to pursue the interests of the Group and other business legitimate reasons.

5.1.8. The Personal Data of the Group Company Shareholders, the Board and senior management shall be kept by the Group's Company Secretary in a secure location which is only accessible by the Group Company Secretariat and legal delegate approved by Chief Legal Officer, with the necessary support of IT. The Company Secretary will confirm to employees of Legal Services (as nominated by the Chief Legal Officer) any changes to this personal data on a 6-monthly basis or sooner if the Company Secretary becomes aware of any changes.

5.1.9. Personal Data of Shareholders or board for each of the Group Companies within the Regions shall be kept by the relevant regional Corporate Secretary or by the regional legal counsel (or delegate) where a regional Corporate Secretary has not been appointed. This data shall be kept in a secure location which is only accessible by the Corporate Secretariat or Legal Department (as applicable), with the necessary support of IT The regional Corporate Secretary or regional legal counsel (or delegate) will confirm any changes to this personal data on a 6-monthly basis or sooner if the Corporate Secretary becomes aware of any changes. This information shall be sent to the Group Corporate Secretary on a 6-month basis, following confirmation of any changes to the Personal Data.

5.1.10. Any requests for information about the Ultimate Beneficial Owners ("UBOs") or any other Know Your Customer ("KYC") requests in relation to the Shareholders of the Company and the board of each of the Group Companies, beneficiaries of the Group and directors, officers and senior management of the Group companies that are received by the Group shall be forwarded to the Group's Corporate Secretary.

5.1.11. The Corporate Secretary shall, if (s)he deems it in the interests of the Group, respond in a prescribed format in a timely manner utilizing the information held pursuant to clause 5.1.6 provided on a 6-monthly basis, or sooner if the Corporate Secretary becomes aware of any changes or contacts relevant Data Subjects.

5.1.12. On a 6-monthly basis, the Corporate Secretary shall notify the Shareholders and Board about the use of the data.

5.1.13. Any Group employees to whom the Corporate Secretary considers it's necessary to assist in processing, storage and management of the Personal Data of the Shareholders and Board of each of the Group Companies, beneficiaries of the Group and directors, officers and senior management of the Group companies acknowledge that they have been advised of this Policy and will comply with it. Lists of persons who are approved to work with such Personal Data shall be kept by the Corporate Secretary. Lists of persons who are compiled by the regional Corporate Secretaries or regional legal counsel (as applicable) to process, store and manage Personal Data in relation to the Group companies managed by the Region shall be maintained by the regional Corporate Secretaries or regional legal counsel (as applicable). Employees that work with such Personal Data or consider that they need to work with such Personal Data shall obtain

the approval of their line Manager to do so and notify the Group Corporate Secretary or the Chief Legal Officer, together with the Head of entity or Region (as applicable). These lists should be copied to the Group Corporate Secretary on a 6-monthly basis.

5.1.14. The Chief Executive Officer and Chief Financial Officer are together authorized to have developed and to approve any further internal procedures, guidance, delegations and templates necessary to ensure the implementation of these clauses 5.1.6 – 5.1.13 inclusive.

Sensitive Personal Data

Only Human Resources personnel and Company-employed medical staff (if applicable) are authorised to process Sensitive Personal Data to pursue a Group Company's legal obligation, responding to government inquiries and ensuring workplace health and safety of Company employees. Prior to processing Sensitive Data, review by the regional Data Protection Officer is required to determine if the processing will impact the rights and freedoms of the Data Subject.

5.1.15. Only the following Sensitive Personal Data can be processed by Group Companies :

a) religious affiliation for withholding tax purposes[3];

b) medical records[4].

5.1.16. Human Resources personnel will conduct such processing in accordance with applicable laws and regulations.

5.1.17. Medical records can be handled only by registered health professionals in accordance with statutory requirements.

5.1.18. 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 accessible to Group Companies that are obliged to process such data under applicable local legislation.

IT related Personal Data

5.1.19. Each Group Companies 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.

5.1.20. If local laws and regulations require an authorisation (e.g., by a data protection or other local authority) for the processing of Personal Data above under 5.1.19 (e.g for Employees IT monitoring), then the Group Companies shall obtain such authorisation in a timely manner.

5.1.21. 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

5.1.22. Employees may also process Personal Data as described in the Information Security policies and procedures and Acceptable Use Policy. The purpose and scope of such processing is further described in those policies.

[3] *Relates for example to 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.)*

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 following[5]:

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 regional Data Protection Contacts 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 a 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, Processors do not need to be disclosed to Data Subjects);

5.2.6 if the Data Controller is an EU or Swiss 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 regional Data Protection Officer or Outside Representative that the Data Subjects may contact regarding their Personal Data;

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 or Swiss entity, the Data Subject's statutory rights; in the European Union for instance, such rights include:

- the right to request access to and rectification or erasure of Personal Data;

- 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 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 are processed, inform the Data Subject of the categories of Personal Data

[5] *Such information may be part of a contract or job application template, etc*.

concerned, the source from which his/her Personal Data originates and if applicable, whether it came from publicly accessible sources.

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 the Regional Data Protection Officer. Response to Data Subjects must occur within one month. However, if the request is complex or the Group Companies receives large number of requests this term may be extended by a further two months.

Automated Decisions[6]

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 request human intervention in any automated processing.

Data Retention

5.4. Employees must retain Personal Data, both electronic and hardcopy, in accordance with the relevant Group Company's policies, and as applicable, the retention schedule approved by the Group CEO set out in Annexure A. The Chief Executive Officer, advised by the Chief Legal Officer, in consultation with the Data Protection Officer, is authorized by the Board to amend the retention schedule from time to time.

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 and the instructions of the competent data protection 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 its discovery; 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 Authority without undue delay and where feasible not later than 72 hours after its discovery. Such notification shall

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

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 among its affiliates and subsidiaries.

5.8. Personal Data will only be disclosed to other Group Companies in accordance with this Policy. 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 Information Security policies and procedures and this Policy.

5.9. Standard contractual clauses should be used to allow possible transfer of personal data between Group Companies.

Sharing of Personal Data with Data Processors

Sharing of Personal Data by Group Companies located in the EU with Data Processors located within the EU or assimilated countries

5.10. If a Group Companies based in the EU wants to share Personal Data with a Data Processor that is based in the EU, the EEA or in a country recognised by the European Commission as ensuring an adequate level of protection[7], the following must occur prior to transferring the data:

5.10.1. there must be a written contract between the Group Company and the Data Processor; and

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 located outside the EU or assimilated countries

5.11. If a Group Company based in EU wants to share Personal Data with a Data Processor 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;

5.11.2. 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 the Group and available from Group Legal;

5.11.3. all transfers of Personal Data must be secure and in compliance with applicable law relating to international data transfers;

5.11.4. the relevant Group Companies exporting the Personal Data must have (i) entered into a set of Standard Contractual Clauses in a form approved by the European Commission with the Data Processor prior to the Personal Data being transferred; and (ii) carry out potential formalities or filings required by its local legislation.

[7] *The European Commission has so far recognised Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay (See http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm for current information).*

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 located outside their home country a local general counsel 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.

Personal Data of Employees Leaving a Group Company

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

5.13.1. give each departing Employee the opportunity to make copies of his/her private Personal Data stored in his/her e-mail in-boxes and corporate computers and mobile computing devices.

5.13.2. deactivate the Employee's corporate e-mail address as soon as reasonably possible after the Employee's departure.

Training Programme

5.14. 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.

5.15. All other Employees will receive training on this Policy upon joining the Company and as needed thereafter.

6. Handling questions, concerns and enquiries

6.1. If an Employee has any questions or concerns in relation to data protection, he/she should contact his/her Data Protection Officer.

6.2. If any Data Subject believes that his/her 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, that complaint must be forwarded without delay to the respective Data Protection Officer.

6.4. The Data Protection Officer will review the complaint on a confidential basis. In the event the Data Protection Officer, the local general counsel will review and forward to the Data Protection Officer as soon as he or she is available.

6.5. Group Companies, with notice to the regional Data Protection Officer, 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.

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.

7. Responsibilities

7.1. The Board is responsible for establishing this Policy.

7.2. The Compliance Department of the respective Region is responsible for:

7.2.1. Providing guidance and advice to the Regional Management 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. Regional Management is 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. Regional Management is responsible for designating a Data Protection Contact and approval and enforcement of respective Region's policies and procedures developed by the Data Protection Officer.

7.5. Data Protection Contacts are responsible for establishing appropriate responsibilities, procedures, training and internal controls within their respective Regions to ensure the consistent implementation of this policy and compliance with its requirements

7.6. It is the responsibility of Regional Management to ensure that their respective employees and Data Processors used are made aware of this policy and that employees processing or having access to Personal Data are periodically trained in data protection requirements.

8. Monitoring

8.1. The Data Protection Officer should, on an annual basis, report on the status of compliance with this Policy to the Compliance Committee of the Board.

8.2. Internal Audit should periodically review compliance with this Policy and report any deficiencies and respective recommendations to the Group Management and the Compliance Committee of the Board.

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 ERG Policy will be updated periodically (but not less than once every 2 years) to reflect any change in the legal and technology environment and in the business requirements.

10.2. All change requests should be directed to one of the Policy Owners or Contacts.

10.3. Material changes to this ERG Policy must be approved by The Board, or if to Appendix A, the Chief Executive Officer.

10.4 Revision 4.0 of this ERG Policy will take effect as from 25 May 2018.

version	Last revision date	Approved by	Date of approval	Comments
1.0	24.08. 2014	The Board	24.08.2014	
1.0	5.05.2015	Compliance	5.05.2015	
2.0	04.03.2016	The Board	13.03.2016	
3.0	20.08.2017	The Board	27.08.2017	
4.0	02.06.2018	The Board	02.06.2018	