RSK GROUP LIMITED

Data Protection Policy

June 2024

1. Introduction

1.1. Protecting the confidentiality, integrity and availability of Personal Data is a critical responsibility that we take seriously at all times.

1.2. This Data Protection Policy ("**policy**") sets out how RSK Group Limited and its subsidiaries ("**RSK Group**") handle the Personal Data of its personnel, customers, contacts and other third parties and should be read in conjunction with our Privacy Policies.

1.3. This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

1.4. The consequences of failing to comply with the Data Protection Legislation include potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, and significant reputational damage.

1.5. **Definitions use in this policy**

1.5.1 The terms in the left-hand column of the following table have the meaning in the corresponding right hand column:

Company	RSK Group Limited or any of its subsidiaries.
Consent	a freely given, specific, informed and unambiguous indication (by way of statement or clear positive action) of the Data Subject's agreement to the Processing of Personal Data relating to them.
Criminal Convictions Data	personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.
Data Controller	the relevant Company that determines when, why and how to process the Personal Data in question.
Data Protection Committee	the committee with responsibility for data protection compliance for the Company (or their delegate from time to time).
Data Protection Legislation	the Data Protection Act 2018 and, for so long as and to the extent that the law of the European Union has legal effect in the UK, the General Data Protection Regulation ((EU) 2016/679) ("EU GDPR"), following which the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) ("DP Brexit Regulations") will take effect (subject to any further changes made during the Brexit transition period), as such legislation may be amended or replaced from time to time.
Data Protection Impact Assessment (DPIA)	a process for the purposes of identifying and minimising data protection risks.
Data Subject	a living, identified or identifiable individual about whom the Company holds Personal Data.
Data Subject Request	a request by a Data Subject to enforce rights listed in paragraph 13 of this Data Protection Policy.

Explicit Consent	consent which requires a very clear and specific statement (that is, not just action).
Lawful basis	The lawful basis of processing information within the 6 categories of Art. 6 EU GDPR.
Information Commissioner's Office (ICO)	the regulatory body in the UK for data protection issues
Personal Data	any information identifying a Data Subject or information relating to a Data Subject that the Company can identify (directly or indirectly) from that data alone or in combination with other identifiers which the Company possesses or can reasonably access. Personal Data includes Special Categories Personal Data. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Company or its third-party service providers put in place to protect it. The accidental or unlawful destruction, loss, alteration, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Personal Data Processing Record	the full and accurate record maintained by the Company of Personal Data Processing.
Personnel	all employees, workers, contractors, agency workers, consultants, directors, managers, members and others who deal with Personal Data in the context of the Company's business.
Privacy Policies	this Data Protection Policy, the Company's other policies, operating procedures or processes related to this policy and designed to protect Personal Data, including the Data Retention Policy and Information Security Policies.
Privacy Notices	separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.
Process or Processing	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Call Recording	The recording of a call on the lawful basis for processing personal information
Special Categories of Personal Data	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

1.6. **Who must comply with this policy?**

1.6.1 This policy applies to all Personnel ("you", "your"). You must read, understand and comply with this policy and our Privacy Policies when Processing Personal Data on the behalf of any RSK Group company and attend training provided on its requirements. This policy sets out what we expect from you for the Company to comply with applicable law.

1.6.2 Any breach of this policy or any other Privacy Policy may result in disciplinary action.

1.7. This policy does not form part of any employee's contract of employment or any contract between a company in the RSK group and any other third party (including clients, customers, referrers, intermediaries and agents).

1.8. **Who is responsible for this policy?**

1.8.1 The Data Controller is responsible for establishing practices and policies in line with the Data Protection Legislation and for ensuring that all those under its control comply with such practices and policies. There are a number of Data Controllers in the RSK Group (see the RSK Group Legal Structure chart in the Company Information section on Oscar).

1.8.2 The RSK Group Limited board of directors, on behalf of all the Data Controllers in the RSK Group, has overall responsibility for this policy and its compliance with our legal and ethical obligations and each Data Controller in the RSK Group has responsibility for compliance with it by their Company and all those under its control.

1.8.3 The Managing Director of each Data Controller in the RSK Group, with support from our Data Protection Committee (details of which are in paragraph 3) shall be responsible for overseeing and monitoring the use and effectiveness of this policy, dealing with any queries about it and for auditing internal compliance control systems and procedures.

1.8.4 The primary and day-to-day responsibility for implementing this policy sits with the Managing Director for each RSK Group Company or business and the Head of each Group Central Function for each of our central support function departments.

1.8.5 The Managing Director of each RSK Group Company or business outside the UK is also responsible for:

1.8.5.1. identifying where local legislation differs from the requirements of this policy; and

1.8.5.2. identifying and implementing arrangements to cover the in-country legislative requirements; and

1.8.5.3. working with our Data Protection Committee to incorporate these differences and identified arrangements into a local policy and our compliance control systems and procedures.

1.8.6 Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it.

1.8.7 On an annual basis, each RSK Group Divisional Director, on behalf of the Data Controllers in their divisions, and the Head of each Group Central Function is required to report to our Data Protection Committee on compliance with this policy in his or her division or central support function department, together with a review of the relevant risk assessment(s), monitoring procedures and recommendations for changes . A summary report of the reports will be submitted to the RSK Group Limited Board for review.

1.8.8 You are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to our Data Protection Committee.

1.9. **How to raise queries or concerns**

1.9.1 You must always contact the Data Protection Committee in the following circumstances:

1.9.1.1. if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see paragraph 3);

1.9.1.2. if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph 3.2.3);

1.9.1.3. if you need to draft Privacy Notices (see paragraph 3.3);

1.9.1.4. if you are unsure about the retention period for the Personal Data being Processed (see paragraph 6);

1.9.1.5. if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 7);

1.9.1.6. if there has been a Personal Data Breach (paragraph 8);

1.9.1.7. if you are unsure on what basis to transfer Personal Data outside the EEA (see paragraph 9);

1.9.1.8. if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 10);

1.9.1.9. whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 11.6) or plan to use Personal Data for purposes other than what it was collected for;

1.9.1.10. if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 11.7);

1.9.1.11. if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 11.5); or

1.9.1.12. if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 11.8).

2. Personal data protection principles

2.1. The Company will adhere to the principles relating to Processing of Personal Data set out in the Data Protection Legislation which require Personal Data to be:

2.1.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

2.1.2 collected only for specified, explicit and legitimate purposes (Purpose Limitation);

2.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

2.1.4 accurate and where necessary kept up to date (Accuracy);

2.1.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Data Retention);

2.1.6 Processed in a manner using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Data Security);

2.1.7 not transferred to another country without appropriate safeguards being in place (Cross Border Transfer Limitation);

2.1.8 processed subject to Data Subject rights and requests in relation to their Personal Data (Data Subject Requests).

2.2. The Company is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

3. Lawfulness, fairness, transparency

3.1. Personal Data must be Processed lawfully, fairly and in a transparent manner.

3.2. **Lawfulness and fairness**

3.2.1 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. Data Protection Legislation restricts the Company's Processing of Personal Data unless there is a lawful basis for such Processing.

3.2.2 Lawful bases for Processing include:

3.2.2.1. the Data Subject has given his or her Consent;

3.2.2.2. the Processing is necessary for the performance of a contract with the Data Subject;

3.2.2.3. the Processing is necessary to meet the Company's legal obligations;

3.2.2.4. the Processing is necessary to protect the Data Subject's vital interests;

3.2.2.5. the Processing is necessary to pursue the legitimate interests of the Company, or third parties provided such interests are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. Where the Company Processes Personal Data based on a legitimate interests basis, the legitimate interests must be set out in appropriate Privacy Notices.

3.2.3 To rely on the consent basis, a Data Subject must indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

3.2.4 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

3.2.5 When processing Special Categories of Personal Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

3.2.6 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Company can demonstrate compliance with Consent requirements.

3.2.7 Where the Company proposes to Process Special Categories of Personal Data or Criminal Convictions Data, additional safeguards must be considered, and additional conditions may need to be satisfied. Special Categories of Personal Data or Criminal Convictions Data relating to Personnel should only be stored by the HR department. You should consult with, and seek approval from, the Data Protection Committee prior commencing any new activity which involves substantial Processing of any Special Categories of Personal Data or Criminal Convictions Data.

3.2.8 The Company must identify and document in its Personal Data Processing Record the legal basis being relied on for each Processing activity. It is your responsibility to notify the Managing Director of your Company or business or the Head of the relevant Group Central Function of any processing for which you have responsibility. It is the responsibility of the Data Controller to record the Processing in the Company's Personal Data Processing Record, a copy of which shall be provided to the Data Protection Committee.

3.3. **Transparency**

3.3.1 The Data Protection Legislation requires the Company to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible and in clear and plain language so that a Data Subject can easily understand them.

3.3.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the Data Protection Legislation including the identity of the Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

3.3.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the Data Protection Legislation as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the Data Protection Legislation and on a basis which contemplates our proposed Processing of that Personal Data.

3.3.4 If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Privacy Policies.

4. Purpose limitation

4.1. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

4.2. You cannot use Personal Data for new, different or incompatible purposes from those disclosed when it was first obtained unless the Company has informed the Data Subject of the new purposes (and the Data Subject Consented, where necessary).

5. Data minimisation and accuracy

5.1. Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which it is Processed. You may only collect, and Process Personal Data required for the purposes of job duties and should not collect excessive data.

5.2. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You must take all reasonable steps to check that the Personal Data the Company uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it was collected.

5.3. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards in accordance with the Company's Data Retention Policy. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

6. Data Retention

6.1. Personal Data must not be kept in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

6.2. You must comply with the Company's Data Retention Policy from time to time which recommends the maximum periods for which Personal Data should normally be retained.

6.3. You must take all reasonable steps to destroy or erase from the Company's systems all Personal Data that the Company no longer requires in accordance with the Company's Data Retention Policy. You should seek the assistance of the Company's IT Department as is appropriate. You should also consider requiring third parties to delete Personal Data where appropriate.

6.4. The Company will inform Data Subjects of the period for which Personal Data is stored in any applicable Privacy Notice.

7. Data Security

7.1. Personal Data must be secured by appropriate technical and organisational measures against

unauthorised or unlawful Processing and against accidental loss, destruction or damage.

7.2. The Company has developed and implemented and will continue to develop and maintain safeguards appropriate to its size, scope and business. The Company will regularly evaluate and test the effectiveness of those safeguards to provide appropriate security for its Processing of Personal Data.

7.3. You are also responsible for protecting the Personal Data the Company holds. You must Process Personal Data in accordance with the Company's policies, instructions and guidance from time to time (including the Company's Information Security Policies) and maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

7.3.1 Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

7.3.2 Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

7.3.3 Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

7.4. You must exercise particular care to protect Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure. Records (including emails containing Special Categories of Personal Data or Criminal Convictions Data) should be password protected and, if transferred, outside of the Company, encrypted where possible.

7.5. You may only transfer Personal Data to third-party service providers who agree to comply with such policies and procedures as the Company requires and which agree to put adequate measures in place.

7.6. You must comply with all instructions in relation to the administrative, physical and technical safeguards or applications the Company maintains to protect Personal Data and must not attempt to circumvent any of them. Failure to comply with such instructions will be dealt with in accordance with the Company's Disciplinary and Dismissal Policy and may result in dismissal.

8. Reporting a Personal Data Breach

8.1. The Data Protection Legislation requires the Company to notify certain Personal Data Breaches to the Information Commissioner's Office (ICO) and, in some instances, the Data Subject. Notification is required within 72 hours.

8.2. Where a Personal Data Breach has occurred or is suspected, you should not attempt to investigate or respond to the incident personally but should immediately notify your Managing Director or, in the Managing Director's absence, the Data Protection Committee. You should preserve all evidence relating to any Personal Data Breach or potential Personal Data Breach.

9. Cross Border Transfer limitation

9.1. The Data Protection Legislation restricts data transfers to countries outside the European Economic Area (EEA) in order to ensure that the level of protection afforded to Data Subjects by the Data Protection Legislation is not undermined. Personal Data is transferred across borders when it is transmitted or sent from the country in which it originates to a different country or when it is viewed or accessed from a different country.

9.2. You may only transfer Personal Data outside the EEA if one of the following conditions applies:

9.2.1 the European Commission has issued a decision confirming that the country to which we transfer the Personal Data provides an adequate level of protection for the Data Subject's rights and freedoms;

9.2.2 appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Protection Committee;

9.2.3 the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

9.2.4 the transfer is necessary for one of the other reasons set out in the Data Protection Legislation including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

9.3. You must comply with any Company's guidelines on cross-border data transfers.

10. Data Subject's Requests

10.1. A Data Subject Request is a request made by or on behalf of a Data Subject to enforce their rights pursuant to Data Protection Legislation.

10.2. Data Subjects have the right to:

10.2.1 **Request access to Personal Data** (commonly known as a "data subject access request"). This enables Data Subjects to receive a copy of the Personal Data the Company holds about them and to check that the Company is lawfully Processing it.

10.2.2 **Request correction of the Personal Data**. This enables Data Subjects to have any incomplete or inaccurate Personal Data the Company holds about them corrected.

10.2.3 **Request erasure of Personal Data**. This enables Data Subjects to ask the Company to delete or remove Personal Data where there is no good reason for the Company continuing to Process it.

10.2.4 **Object to processing of Personal Data**. Where the Company is relying on a legitimate interest (or that of a third party) as a lawful basis for Processing and there is something about a particular situation which makes the Data Subject want to object to Processing on this ground.

10.2.5 **Request the restriction of Processing of Personal Data**. This enables Data Subjects to ask the Company to suspend the Processing of Personal Data about them, for example, if the Data Subject wants the Company to establish its accuracy or the reason for Processing it.

10.2.6 **Request the transfer** of certain categories of Personal Data to another party.

10.3. If Data Subjects wish to exercise the above rights in relation to Personal Data they should submit their request, normally in writing, to the Data Protection Committee using the contact details at the end of this policy. We ask that Data Subjects complete our Data Subject Access Request Form which is available on request. This is help us deal with your request more easily. Only Personnel authorised by the Data Protection Committee shall respond to Data Subject Requests.

10.4. Data Subject Requests must receive a prompt response to be issued no later than one month after the date on which the request is received. This can be extended in limited circumstances as advised by the Data Protection Committee.

10.5. The Company shall not charge a fee when responding to a Data Subject Request, unless the request is unfounded or excessive. In such instances, the Company may charge a reasonable fee that takes into account the administrative costs of taking the necessary action to respond. Where request is unfounded or unreasonable, the Company may also refuse to act on the request.

10.6. In limited circumstances, the Company may be exempt from complying (in whole or in part) with the Data Subject Request. Exemptions may apply, for example, for reasons relating to the public interest, the prevention of crime or for reasons relating to legal proceedings.

10.7. The Company is required to respond to a Data Subject Request in relation to Personal Data held at the time the request was received. Under no circumstances should you amend or delete Personal Data other than in the ordinary course of business once a Data Subject Request has been received.

11. Accountability

11.1. The Company must implement appropriate technical and organisational measures in an effective manner to maintain compliance with data protection principles. The Company is responsible for, and must be able to demonstrate, compliance with the data protection principles.

11.2. Record keeping

11.2.1 The Company keeps full and accurate records of all its data Processing activities (Personal Data Processing Record).

11.2.2 You must assist the Company in keeping and maintaining an accurate Personal Data Processing Record reflecting the Company's Processing.

11.2.3 In relation to Data Processing under your control, you must provide your Managing Director or Head of Group Central Function with requested details including: clear descriptions of the types of Personal Data, categories of Data Subjects, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, Personal Data retention periods and a description of the security measures in place.

11.3. Call Recording

11.3.1 RSK Group has a telephone system that is capable of recording conversations. As with most companies this is standard practice that allows the recording of telephone calls for training, monitoring, compliance and security purposes.

11.3.2 You will be advised at the start of any call if the call is being recorded. Personal data collected in the course of the recorded activities will be processed fairly and lawfully (see paragraph 3.3) in accordance with EU GDPR.

11.3.3 Call recordings will be turned off, if you are required to provide your credit/debit card details, in line with Payment Card Industry Data Security Standards (PCS DSS).

11.3.4 Call recordings will be held for a period of time (see Data Retention Policy) subject to it not being needed for ongoing quality and control purposes or criminal actions.

11.4. **Training and audit**

11.4.1 You are required to complete all data privacy related training and are responsible for ensuring that your team completes the mandatory training in accordance with the Company's training requirements.

11.4.2 You must regularly review all the systems and processes under your control to check that they comply with this policy and that adequate governance controls and resources are in place to monitor the proper use and protection of Personal Data.

11.5. **Direct marketing**

11.5.1 The Company is subject to certain rules and privacy laws when marketing to its customers.

11.5.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

11.5.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

11.5.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to enable marketing preferences to be respected in the future.

11.5.5 You must inform the Group Marketing Director before engaging in any direct marketing and follow any guidance issued by the Group Marketing Department and/or Data Protection Committee.

11.6. **Privacy by Design and Data Protection Impact Assessment**

11.6.1 The Company is required to implement appropriate and effective technical and organisational measures when Processing Personal Data.

11.6.2 You must assess what measures can be implemented in relation to all systems and processes in your area of responsibility which Process Personal Data by taking into account the nature, scope, context and purposes of Processing, the risks of likelihood and severity of harm to Data Subject’s rights posed by the Processing, the state of the art and the cost of implementation.

11.6.3 A formal Data Protection Impact Assessment (DPIA) is mandatory where proposed Processing is likely to result in a high risk of harm to Data Subject’s rights either because there is a high probability of some harm or a lower possibility of serious harm. High risks are likely to arise where Processing involves, for example, use of new technologies, largescale Processing (particularly of Special Categories of Personal Data or Criminal Convictions Data), profiling and tracking Data Subject’s location or behaviours, automated decision, making or combining or matching data from multiple sources.

11.6.4 Where a DPIA is required, this must be prepared, discussed with and approved by the Data Protection Committee. A DPIA must include:

11.6.4.1. a description of the Processing, its purposes and the legitimate interests relied on, if

appropriate;

11.6.4.2. an assessment of the necessity and proportionality of the Processing in relation to its purpose;

11.6.4.3. an assessment of the risk to Data Subjects; and

11.6.4.4. the risk mitigation measures in place and demonstration of compliance.

11.7. **Automated Processing (including profiling) and Automated Decision-Making**

11.7.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

11.7.1.1. a Data Subject has Explicitly Consented;

11.7.1.2. the Processing is authorised by law; or

11.7.1.3. the Processing is necessary for the performance of or entering into a contract.

11.7.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds 11.7.1.2 or 11.7.1.3 will not be allowed but the Special Categories of Personal Data or Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

11.7.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

11.7.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

11.7.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

11.8. **Sharing Personal Data**

11.8.1 Generally, the Company is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

11.8.2 You may only share the Personal Data the Company holds with another employee, agent or representative of the Company if the recipient has a job-related need to know the information.

11.8.3 You may only share the Personal Data the Company holds with third parties, such as the Company service providers, if:

11.8.3.1. they have a need to know the information for the purposes of providing the contracted services;

11.8.3.2. sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

11.8.3.3. the third party has agreed to comply with any required data security standards, policies and procedures and put adequate security measures in place;

11.8.3.4. the transfer complies with any applicable cross border transfer restrictions; and

11.8.3.5. a fully executed written contract that contains approved third party clauses has been obtained.

12. Changes to this policy

12.1. We keep this policy under regular review and reserve the right to change it at any time. It is your responsibility to ensure that your knowledge of this policy is up to date and that you comply with its terms.

12.2. This policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

13. Data Protection Committee

13.1. The Data Protection Committee members are:

13.1.1 Legal & Compliance Counsel;

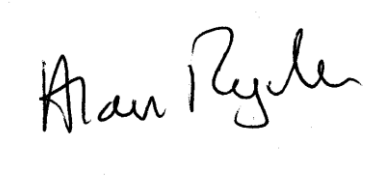
13.1.2 Group HR Director;

13.1.3 Business Systems Manager; and

13.1.4 Group Marketing Director.

13.2. Contact the Data Protection Committee by emailing ***privacy@rsk.co.uk*****.**

This Policy has been approved and adopted by the RSK Group Limited Board.



……

Alan Ryder, Chief Executive

Date: 27 June 2024