Data Protection Policy

Contents

1 Introduction

RTC Group Plc, referred to throughout this document as RTC, have implemented the following Data Protection Policy in accordance with ISO 27001:2013, the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulations (together referred to as the 'Data Protection Laws'), to ensure that all Personally Identifiable Information controlled or processed by us or our subcontracted third parties, is secure, its integrity is maintained and it is retained in accordance with an individual's rights.

The RTC Group Plc governs the following companies with this policy.

Company Name	Registered Address	Registration Number
RTC Group Plc	The Derby Conference Centre, London Road, Derby, DE24 8UX	02558971
The Derby Conference Centre Limited	The Derby Conference Centre, London Road, Derby, DE24 8UX	03061642
ATA Recruitment Limited	The Derby Conference Centre, London Road, Derby, DE24 8UX	04315383
Ganymede Solutions Limited	The Derby Conference Centre, London Road, Derby, DE24 8UX	03579773
ATA Global Staffing Solutions Ltd	The Derby Conference Centre, London Road, Derby, DE24 8UX	03125335

The General Data Protection Regulation 2018 (GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.1 Definitions used by the RTC Group of companies (drawn from the GDPR)

Material scope (Article 2) **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. electronically) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) **–** the GDPR will apply to all controllers and processors that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers and processors outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

1.2 Definitions

Data controller ('Controller')– the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. **The RTC Group and its subsidiary companies are Data Controllers.**

Data Processor ('Processor') – the natural or legal person, public authority, agency or other body which deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing. **The RTC Group and its subsidiary companies are Data Processors.**

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

Establishment – the main establishment of the data controller in the EU will be the place in which the data controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities. **The main establishments of the RTC Group, ATA Recruitment, Ganymede Solutions, and The Derby Conference Centre are located in Derby, England. The main establishment for ATA Global Staffing Solutions is Birmingham, England.**

Personal data – 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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data subject – any living individual who is the subject of personal data held by an organisation.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2 Policy Statement

The RTC Group and the management teams of all subsidiary companies, are committed to compliance with all relevant UK, EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information the RTC Group collects and processes in accordance with the applicable Data Protection Laws.

Our overall objective is;

"To protect the rights of all individuals (data subjects), of whom we hold data and ensure that the Personally Identifiable Information is kept in a secure Environment with its integrity maintained."

The RTC Group and the management teams of all subsidiary companies will implement the controls associated with the RTC Information Security Management System, or company specific Data Protection Procedures throughout the organisation, irrelevant of location.

Compliance with the GDPR is described by this policy and other relevant processes such as the RTC Group Information Security Management Manual along with connected processes and procedures as detailed within our Information Security Management System.

The EU GDPR and this policy apply to all RTC Group companies' personal data processing functions, including those performed on Prospective candidates', successful candidates', agency workers', employees, suppliers' and clients' personal data, and any other personal data the RTC Group of companies process from any source.

The RTC Group and the management teams of all group companies have established objectives for data protection, information security and privacy, which are managed in accordance with our strategic business goals.

The objectives and targets are based on the Information Assets recorded in the Information Asset register.

The RTC Group have appointed a Group Data Protection Representative (DPR) who is responsible for reviewing the registering of Information Assets Register annually ensuring that any operational data changes are mitigated by means of data protection risk assessment.

The company specific data within the Information Asset Register is managed at a company level and reviewed periodically by the DPR and the Information Security Manager.

This policy applies to employees, staff, and interested third parties of RTC Group companies, including outsourced suppliers or data processors. Any breach of the EU GDPR or our Group Information Security Management System will be dealt with under RTC Group disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for any RTC Group companies and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by any RTC Group company without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which any RTC Group company is committed, and which gives any RTC Group company the right to audit compliance with the agreement.

3 Responsibilities

The companies under the control and management of the RTC Group have been classified as both Data Controllers and Data Processors under the EU GDPR.

Senior Management and all those in managerial or supervisory roles in any RTC Group company are responsible for developing and encouraging good information handling practices within the companies; responsibilities are set out in individual job descriptions. As a minimum the following responsibilities apply;

3.1 RTC Group Data Protection Representative (DPR)

- Development and implementation of the GDPR controls as required by this policy
- Security and risk management in relation to compliance with the policy.
- Discharge of any activities required by this policy that are not owned directly by them.
- Investigation of any breaches or incidents.
- Reporting to the Board and all group companies any possible trends or performance issues

3.2 Company Data Protection Representative (DPR)

- Being the first point of call for any queries associated with GDPR compliance
- Ensuring a process is in place to communicate GDPR compliance implications, risks and consequences.
- Management of Subject Access Requests and reporting to the Group DPR / board their successful implementation.
- Assisting the Group DPR with the investigation of any breaches or incidents
- Reporting of possible trends or performance issues to the Group DPR.

3.3 Information Security Manager

- Management of the infrastructure, policies and procedures required to maintain the security and integrity of any personal data held any RTC Group company.
- Communication of risks or opportunities associated with information security and integrity to the Group DPR
- Investigation of any breaches where security or integrity is in question.
- Reporting of possible trends or performance issues to the Group DPR.

3.4 All RTC Group Employees

- Implementation of this policy and associated procedures
- Reporting of any risks or opportunities to the DPR
- Assisting the DPR with the implementation of the Subject Access Request Procedure
- Assisting the DPR with the investigation of any possible breaches or incidents.

4 Data Protection Principals

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the EU GDPR. The RTC Group policies and procedures are designed to ensure compliance with the principles and relevant Data Protection Laws.

4.1 Personal data must be processed lawfully, fairly and transparently

4.1.1 Lawful

The RTC Group of companies will identify the lawful basis by which we process personal data. These are recorded within the relevant Information Asset Register. We will also highlight the Legal basis for main Personal Information types within our Privacy Notice.

4.1.2 Fairly

In order for processing to be fair, the RTC Group of companies will make certain information available to the data subjects as far as reasonably practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources. This includes any possible profiling or automatic decision making such as candidate selection through minimum requirements.

4.1.3 Transparently

The RTC Group of companies will ensure that the data we control and process is managed transparently through the implementation of our Privacy Notices.

The following Privacy Notices will be made available as a minimum;

- Operational Privacy Notices

- Prospective Employee / Employee and Third-Party Privacy Notice
- Website Privacy Notice

As a minimum, we will provide, upon receipt of a Subject Access Request;

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the DPR;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

All Subject Access Requests will be carried out in accordance with the relevant Subject Access Request procedure, which is managed by the company specific DPR. The Subject Access Request process is monitored and where necessary managed by the RTC Group DPR.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

The RTC Group of companies will ensure that data obtained for specified purposes will not be used for any purpose other than those formally notified to the data subjects.

The primary purpose for collecting **candidate** data is to assist a candidate in finding work.

The primary purpose of collecting **employee** data is to ensure that they are employed in a legal and supportive manner that encourages development and loyalty.

The primary purpose of collecting **customer, client, prospective client, supplier or prospective supplier** data is to establish relationships and manage contractual requirements.

During normal operations, RTC Group of companies collect some or all of the following types of personal data. The following list is meant as an example and is not exhaustive.

- Application forms
- Recruitment documentation (interview notes, assessments etc.)
- Personal details (address, contact details, date of birth etc.)
- Payroll information
- Equality and diversity monitoring forms
- Medical records
- Sickness absence records
- Attendance records
- Records of disciplinary/grievance proceedings
- Unspent criminal convictions records
- Personnel files relating to former employees
- Guest / event attendee records
- Guest / attendee allergy information

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

The RTC Group DPR, with the support of the company specific DPR, ensures that the RTC Group of companies do not collect information that is not strictly necessary for the purpose for which it is obtained.

The RTC Group ensures that any individual requested to provide personal information, whether candidate, employee, customer or client, prospective customer or client, supplier, prospective supplier or any other data subject is given access to the relevant Privacy Notice to fully inform them of their rights and how we plan on managing their personal information.

The RTC Group DPR ensures that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

All data stored by the RTC Group of companies is periodically reviewed and updated as necessary. No data will be kept unless it is reasonable to assume that it is accurate. Data retention periods are detailed in the Data Retention Procedure and are recorded against individual Information Assets within the Information Assets Register.

The RTC Group DPR is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the data subject to ensure that data held by the RTC Group of companies is accurate and up to date.

Employees are required to notify the Group HR department of any changes in circumstance to enable personal records to be updated accordingly.

The Company DPR is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the RTC Group DPR will review with each of the companies the retention dates of all the personal data processed. The details of the retention requirements are recorded in the Information Assets Register. Any data that needs to be deleted / destroyed will be done so in accordance with company specific Record Retention Procedure and the RTC Information Security Management Policy.

The Company DPR is responsible for ensuring that the rectification processes are in place and performing effectively. This will ensure that all staff / consultants are able to rectify information within a 28 day period of being informed. The 28 day period has been selected as the preferred timescale due to it being the shortest calendar month in the year. This can be extended to a full calendar month if necessary and a further two months for justifiably complex requests. If any of the RTC Group of companies decides not to comply with the request, the RTC Group DPR will respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

The Company DPR is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Personal data will be retained in line with the company specific Record Retention Procedure and the Information Asset Register. Once it's retention date is passed, it must be securely destroyed in accordance with the Information Security Management Manual.

The RTC Group DPR along with the relevant Managing Director specifically approves any data retention that exceeds the retention periods defined in the Record Retention Procedure and Information Asset Register. In addition to this, any justification is clearly identified and in line with the requirements of the data protection legislation. This approval will be written and recorded within the Information Asset Register. Should Personal data be retained, a justification will be logged detailing any necessary restrictions.

4.6 Personal data must be processed in a manner that ensures appropriate security

The security of all data will be managed in accordance with RTC Group Information Security Management System, which has been developed in accordance with ISO 27001:2013.

The RTC Group DPR, the Information Security Manager and the relevant Managing Director will risk assess all types of data held by the RTC Group, taking into account all controlling or processing operations.

In determining appropriateness, the RTC Group DPR, the Information Security Manager and the relevant Managing Director will also consider the extent of possible damage or loss that might be caused to individuals (e.g. candidates, employees, customers, 3rd parties, etc.) if a security breach occurs, the effect of any security breach on any of the RTC group of companies, and any likely reputational damage including the possible loss of stakeholders' trust.

When assessing appropriate technical measures, the RTC Group DPR, the Information Security Manager and the relevant Managing Director will consider, as a minimum, the following:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave RTC Group companies premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to the activities and locale.

When assessing appropriate organisational measures the RTC Group DPR, the Information Security Manager and the relevant Managing Director will consider the following:

- The appropriate training levels throughout each company
- Measures that consider the reliability of employees (such as references etc.);
- The expected retention period of employees.;
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules and protocols about passwords;

- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA (where applicable).
- Ensuring that appropriate contracts, Binding Corporate Rules (BCR's) and/or model contract clauses are in place to govern the activities of any third party or international processing that takes place.[1]

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

Additional controls can be found in RTC Group Information Security Management Manual.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The RTC Group of companies demonstrate compliance with the data protection principles by implementing data protection policies, adhering to best practice, implementing technical and organisational measures, following our Information Security Management Manual as well as adopting techniques such as data protection by design, Information Risk Assessments, breach notification procedures and incident response plans.

5 Data Subjects Rights

The RTC Group ensures that the rights of all Data Subjects are met with regards to processing and control of their personal data.

These rights are:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-making processes that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated processes.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the Information Commissioners Office, (ICO) to assess whether any provision of the EU GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

The RTC Group of companies ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure.
- Data subjects have the right to complain to the RTC Group or any of the RTC Group companies relating to the processing of their personal data, the handling of a request from a data subject and

[1] Binding Corporate Rules and Model Contract Clauses are the minimum controls required by the EU GDPR when an organization has affiliates working in countries outside of the EAA.

appeals from a data subject on how complaints have been handled in line with the Data Handling Complaints Procedure.

6 Consent and Permissions

RTC Group companies understand 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

RTC Group companies understand 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

RTC Group companies will seek consent from all Data Subjects where there is not pre-determined legitimate or legal basis for retaining data in accordance with our Document Control Procedure, Record Retention Procedure and Information Assets register.

RTC Group companies understands 'permission' to mean that it has been freely given for any activities that we have a legitimate business use.

For special categories of personal data, explicit written consent of data subjects is obtained unless an alternative legitimate basis for processing exists.

7 Security of Data

All Employees are responsible for ensuring that any personal data that RTC Group companies hold and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the RTC Group companys to receive that information and has entered into a confidentiality agreement and legally binding contract.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy as detailed within the Information Security Management Manual.

All security and integrity of all data is managed in accordance with the RTC Group Information Security Management Manual.

8 Disclosure of data

The RTC Group of companies ensure that personal data is not disclosed to unauthorised third parties, unless there is a lawful reason to do so.

All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the RTC Group of companies' activities.

The RTC Group of companies may have a legal obligation to disclose personal data to Government authorities or for crime prevention purposes or in relation to national security.

9 Retention and disposal of data

The RTC Group shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

The RTC Group may store data for longer periods if the personal data will be processed solely for archiving purposes, in the public interest or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be recorded in the Information Asset Register.

Data outside of the retention dates will be disposed of in accordance with the RTC Group Information Security Management Policy.

All Personal data is disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

In the event that a Data Subject wishes for their data to be erased in its entirety, the RTC Group of companies will highlight the risk that they may be contacted again if we do not keep a record of their wishes to be erased.

10 Data transfers

The RTC Group of companies acknowledge that all exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the following specified safeguards, or exceptions, apply, or consent has been received from the Data Subject based on communication of the risks.

10.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.2 Privacy Shield

Information assets processed in the US are processed with organisation signed up with the Privacy Shield framework at the U.S. Department of Commerce (DOC). Should there be requirements for new data processors to be introduced (for example if data was stored in a hosted server), the RTC Group of companies will check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce (DOC).

The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

11 Assessment of adequacy by the data controller

ATA Global Staffing Solutions are the only subsidiary that shares Information Assets with data controllers outside of the European Economic Area, (EAA) If Consent cannot be received, based on all risks communicated, then they will make an assessment of adequacy.

The assessment of adequacy, as a minimum will address;

- the nature of the information being transferred;
- the country or territory of the origin, and final destination of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location

11.1 Binding corporate rules

The RTC Group of companies may adopt binding corporate rules, approved for use by the RTC Group, for the transfer of data outside the European Economic Area (EAA) to another RTC Group entity.

11.2 Model contract clauses

The RTC Group of companies may adopt approved model contract clauses, as defined within the EU GDPR for the transfer of data outside of the EEA. If the RTC Group adopts the model contract clauses approved by the Board, there is an automatic recognition of adequacy.

11.3 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defense of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12 Information asset register/data inventory

RTC Group of companies have implemented an Information Asset Management register that is maintained by the Company DPR. The register headings are:

- Asset number or ID
- Name of asset
- What does it do
- Asset type
- Information Classification
- Data collection activity

- Location
- Primary Department
- Owner
- Volume
- Information Category
- Contains Personal data
- Data processor
- Access
- Shared Format
- Retention
- Risks / impact
- GDPR Use Justification
- Risk Assessment
- Transferred outside of the EAA

The RTC Group of companies are aware of all risks associated with the processing and control of the data detailed within the Information Asset Register.

The RTC Group assess level of risk to individuals associated with the processing of their personal data in accordance with the RTC Group Asset Data Risk Assessment procedure.

Where a type of processing, in particular using new technologies and 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 natural persons, the RTC Group of companies shall, prior to the processing, conduct a Data Protection Risk Assessment to identify if existing mitigations are acceptable and the risk consequences / likelihoods are reduced to an acceptable level.

Where the resultant consequences or likelihoods are not deemed to be acceptable, the DPR and the relevant Managing Director will establish new actions / mitigations to be implemented prior to the processing activities.

The DPR shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Board.

13 Related Policies and Procedures

- RTC Group Disciplinary Procedure
- Company Specific Privacy Notices
- RTC Information Security Management Manual

If you have any queries relating to this policy or enquiries or complaints, please contact The Group HR Department.