Data Protection Policy

'Five Rivers is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment'

Policy Owner	DPO
Authoriser	C.O.O
Date of Original Issue	27 June 2018
Date of Last Review	01/09/2025
Date of Next Review	01/09/2026
Version	V3

Table of Contents

Change record

Date	Author	Version	Reason for change
June 2018	Kate Bradbury, Company Secretary	2	Amend for the GDPR and DPA 2018.

1. Data Protection Policy

1.1 Policy Statement

This Data Protection Policy sets out how Five Rivers Child Care Limited and its Group Companies ("we", "our", "us", "the Five Rivers Group") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Data Protection 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.

This Data Protection Policy applies to all Five Rivers Group Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Five Rivers Group to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

1.2 Terms and Definitions

The below table sets out a number of terms and definitions used within this document:

Term	Definition
Automated Decision-Making (ADM)	when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. UKGDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Five Rivers Group Personnel	all employees, workers contractors, agency workers, consultants, directors, members and others.
Consent	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Term	Definition
Data Controller	the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Five Rivers Group Personnel and Personal Data used in our business for our own commercial purposes.
Data Subject	a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
Data Privacy Impact Assessment (DPIA):	tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.
Data Protection Measures	the measures that all of the Five Rivers Group's employees, agents, contractors, or other parties working on its behalf must comply with when working with personal data.
Data Protection Officer (DPO)	the person required to be appointed in specific circumstances under UKGDPR. Where a mandatory DPO has not been appointed, this term means the Chief operating officer (COO)
EEA	the 27 countries in the EU, and the 3 EFTA states (Iceland, Liechtenstein and Norway)
Explicit Consent	consent which requires a very clear and specific statement (that is, not just action).
United Kingdom General Data Protection Regulation (GDPR):	UKGDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679).
Group	means, in relation to any Five Rivers Group, that Five Rivers Group and any other Five Rivers Group which, at the relevant time, is its Holding Five Rivers Group or Subsidiary, or the Subsidiary of any such Holding Five Rivers Group; and "Member" of a Group has a corresponding meaning.
Holding Five Rivers Group	has the meanings given to this expression by Sections 736 and 736A of the Companies Act 1985.
Organisational Measures	the measures to be taken by the Five Rivers Group with respect to the collection, holding and processing of personal date and set out in Appendix B to this Data Protection Policy.
Personal Data	any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address,

Term	Definition
	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 we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
Privacy Guidelines	the Five Rivers Group privacy/GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available on the intranet, Connect.
Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies	separate notices setting out information that may be provided to Data Subjects when the Five Rivers Group collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose and are available on Connect.
Processing or Process	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.
Pseudonymisation or Pseudonymised	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Related Policies	the Five Rivers Group's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on Connect as updated from time to time.
Sensitive 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, and Personal Data relating to criminal offences and convictions.
Subsidiary	has the meanings given to this expression by Sections 736 and 736A of the Companies Act 1985;

1.3 Data Protection

Five Rivers Child Care supports the objectives of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and other legislation relating to Data Processing, including the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Freedom of Information Act 2000. Five Rivers Child Care has a statutory obligation to process personal data in accordance with the provisions of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
Every member of Five Rivers Child Care has an obligation to ensure that the information they process (use) is collected, maintained and disclosed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and the Five Rivers Child Care Data Protection Policy.

1.4 Disclosure of Information

Any use or disclosure of information held within Five Rivers Child Care, without there being a legitimate purpose or legal basis, will be classed as unauthorised and is a criminal offence under section 170 (unlawful obtaining ect. of personal data) DPA 2018.

1.5 Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Five Rivers Group is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All departments, are responsible for ensuring all of their Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines and ensuring the implementation of and compliance with the Data Protection Measures and Operational Measures. That post is held by the Head of Contracting and Service Development, who can be contacted by email to DPO@five-rivers.org

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Five Rivers Group) (see section 1.7 below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see section 1.7.2 *General* below);

(c) if you need to rely on Consent and the Data Subject is a child (see section 1.7.2 *Children* below);

(d) if you need to draft Privacy Notices or Fair Processing Notices (see section 1.7.3 below);

(e) if you are unsure about the retention period for the Personal Data being Processed (see section 1.11 below);

(f) if you are unsure about what security or other measures you need to implement to protect Personal Data (see section 1.12.1 below below);

(g) if there has been a Personal Data Breach (see section 1.12.2 below);

(h) if you are unsure on what basis to transfer Personal Data outside the EEA (see section 1.13 below);

(i) if you need any assistance dealing with any rights invoked by a Data Subject (see section 1.14 below);

(j) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see section 1.18 below below) or plan to use Personal Data for purposes others than what it was collected for;

(k) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see section 1.19 below);

(l) If you need help complying with applicable law when carrying out direct marketing activities (see section 1.20 below); or

if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our customers (see section 1.21 below).

1.6 Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

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

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) 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 (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

1.7 Lawfulness, fairness, transparency

1.7.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

You must identify and document the legal ground being relied on for each Processing activity on Connect.

1.7.2 Consent

General

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they 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.

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.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to

Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Five Rivers Group can demonstrate compliance with Consent requirements.

Children

The GDPR sets out specific requirements for obtaining consent from children. Where a child is below the age of 16, the consent of the holder of parental responsibility is required unless it is for preventative or counselling services being directly offered to the child (Recital 38 UKGDPR).

Children have the same data protection rights as adults and can exercise them independently if they are competent to do so. Parents or guardians may exercise the rights of the child when the child is not capable of doing so or it's in demonstrably best interests of the child. A child can authorized an appropriate third party to exercise their rights on their behalf

1.7.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers 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 or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them and which must be presented when the Data Subject first provides the Personal Data (where data is collected directly) and as soon as possible after collecting/receiving the data (where data is collected indirectly.

All Privacy Notices and Fair Processing Notices to be issued must be in the Five Rivers Group standard form which is available on Connect.

1.8 Purpose limitation

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.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

1.9 Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Five Rivers Group's data retention guidelines.

1.10 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

1.11 Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

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

The Five Rivers Group will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Five Rivers Group's Data Retention Policy.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Five Rivers Group's applicable records, retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

1.12 Security integrity and confidentiality

1.12.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

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

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

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

You must [comply with all applicable aspects of the Five Rivers Group's BYOD Policy and IT Security Policy which is available on Connect and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data].

1.12.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches the DPO, the information technology or security department, the legal department and follow the Data Breach Reporting Plan set out in the Schedule. You should preserve all evidence relating to the potential Personal Data Breach.

1.13 Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country. Five rivers doesn't allow the transfer of data outside the EEA unless in exceptional circumstances that need to be confirmed by the DPO who will advise further.

1.14 Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your supervisor and the DPO and comply with the Five Rivers Group's Data Subject response process.

1.15 Accountability

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

The Five Rivers Group must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

(d) regularly training Five Rivers Group Personnel on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Five Rivers Group must maintain a record of training attendance by Five Rivers Group Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

1.16 Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Five Rivers Group's record keeping requirements as communicated to you from time to time.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

1.17 Training and audit

We are required to ensure all Five Rivers Group Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the Five Rivers Group's GDPR training requirements as communicated to you from time to time.

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

1.18 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and ADM;

(c) large scale Processing of Sensitive Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

1.19 Automated Processing (including profiling) and Automated Decision-Making

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

(a) Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

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.

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.

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

Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Five Rivers Group's requirements on profiling or ADM as communicated to you from time to time.

1.20 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

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.

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.

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 ensure that marketing preferences are respected in the future.

1.21 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding Five Rivers Group along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) 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;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with the Five Rivers Group's requirements on sharing data with third parties.