REDDO CARE & SUPPORT CIC

GDPR Policies

- *Privacy Policy*
- *Data Protection Policy*
- *Data Retention Policy*
- *GDPR Compliance Statement*
- *Statement of Processing (Customers)*
- *Data Processing Notice (by consent)*
- *Data Processing Notice (legitimate basis)*

PRIVACY POLICY

Reddo Care & Support CIC is committed to ensuring that your privacy is protected. This policy explains how Reddo Care & Support CIC uses any information collected about you.

We will collect and process the following data about you:

The data collected allows Reddo Care & Support CIC to contact you to update you with any service changes or items that may be of interest to you.

Information you give us may include your name, address, e-mail address and phone number, details about your employment history, skills or qualifications, and other information you choose to share with us.

This is information about you that you give us by filling in forms on our site or by corresponding with us by phone, e-mail or otherwise. It includes information you provide when you register to use our site, subscribe to our service, participate in discussion boards or other social media functions on our site (if any), enter a competition, promotion or survey, request further information, propose ideas to us, and when you report a problem with our site.

Information we collect about you with regard to each of your visits to our site we will automatically collect the following information:

- **Technical information**, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information (if any), browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;
- **Information about your visit**, including the full Uniform Resource Locators (URL), clickstream to, through and from our site (including date and time), pages you viewed or things you searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page, and any phone number used to call us.
- **Information we receive from other sources**. This is information we receive about you if you use any of the other websites we operate or the other services we provide. We are working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies). We will notify you when we receive information about you from them and the purposes for which we intend to use that information.

Cookies

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. For detailed information on the cookies we use and the purposes for which we use them see our Cookie Policy.

We use information held about you in the following ways:

- to carry out our obligations arising from any contracts entered into between you and us and to provide you with the information, products and services that you request from us;
- to provide you with information about other products and services we offer that are similar to those that you have already purchased or enquired about;
- to provide you, or permit selected third parties to provide you, with information about goods or services we feel may interest you. If you are an existing customer, we will only contact you by electronic means (e-mail or SMS) with information about goods and services similar to those which were the subject of a previous sale or negotiations of a sale to you. If you are a new customer, and where we permit selected third parties to use your data, we (or they) will contact you by electronic means only if you have consented to this. If you do not want us to use your data in this way, or to pass your details on to third parties for marketing purposes, please tick the relevant box situated on the form on which we collect your data (the registration form or processing notice or similar document provided to you);
- to notify you about changes to our service;
- to ensure that content from our site is presented in the most effective manner for you and for your computer.
- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to allow you to participate in interactive features of our service, when you choose to do so;
- as part of our efforts to keep our site safe and secure;
- to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you;
- to make suggestions and recommendations to you and other users of our site about goods or services that may interest you or them.

Information we receive from other sources.

We will combine this information with information you give to us and information we collect about you. We will use this information and the combined information for the purposes set out above (depending on the types of information we receive).

Disclosure of Your Information

You agree that we have the right to share your personal information with:

- Selected third parties including:
- business partners, suppliers and subcontractors for the performance of any contract we enter into with them or you;
- analytics and search engine providers that assist us in the improvement and optimisation of our site;
- credit reference agencies for the purpose of assessing your credit score where this is a condition of us entering into a contract with you.

Your Rights

You have the right to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also exercise the right at any time by contacting us at office@reddocares.org.uk.

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to the office@reddocares.org.uk

DATA PROTECTION POLICY

1. Interpretation

1.1. Definitions:

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. The UK GDPR 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.

Company name: Reddo Care & Support CIC

Company 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.

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 UK GDPR. We are the Data Controller of all Personal Data relating to our Company 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 Officer (DPO): the person required to be appointed in specific circumstances under the UK GDPR. Where a mandatory DPO has not been appointed, this term means a **Data Protection Manager (DPM**) or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK General Data Protection Regulation (UK GDPR): is based on the EU GDPR (General Data Protection Regulation (*(EU) 2016/679*)) which came into effect on 25 May 2018 and applied in the UK until 1 January 2021. EU GDPR was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU, it sits alongside and supplements the UK GDPR. Personal Data is subject to the legal safeguards specified in the UK GDPR.

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, 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 UK GDPR.

Privacy Guidelines: the Company privacy/UK GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies

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 Company 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.

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 Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data

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.

2. Introduction

2.1. This Data Protection Policy sets out how Reddo Care & Support CIC ("we", "our", "us", "the Company", “Reddo”) handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

2.2. 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.

2.3. This Data Protection Policy applies to all Company 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 Company 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.

2.4. 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 DPM.

3. Scope

3.1. 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 Company is exposed to potential fines of up to EUR 20 million (approximately £18 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 UK GDPR.

3.2. All CEOs, MDs, individual business areas/units/departments, supervisors, and managers are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.3. The DPM is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Georges Debbas, Data Protection Manager (DPM), E: office@reddocares.org.uk

3.4. Please contact the DPM with any questions about the operation of this Data Protection Policy 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 DPM 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 Company);

(b) if you need to rely on Consent and/or need to capture Explicit Consent;

(c) if you need to draft Privacy Notices or Fair Processing Notices;

(d) if you are unsure about the retention period for the Personal Data being Processed;

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data;

(f) if there has been a Personal Data Breach;

(g) if you are unsure on what basis to transfer Personal Data outside the EEA;

(h) if you need any assistance dealing with any rights invoked by a Data Subject;

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

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;

(k) if you need help complying with applicable law when carrying out direct marketing activities; or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our customers and suppliers).

4. **Personal data protection principles**

We adhere to the principles relating to Processing of Personal Data set out in the UK 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).

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

5. Lawfulness, fairness, transparency

5.1. Lawfulness and fairness

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

5.1.2. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK 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.

5.1.3. The UK 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 te Data Subject;

(c) to meet our legal compliance obligations;

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

(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; or

(f) with consent.

5.1.4. You must identify and document the legal ground being relied on for each Processing activity in accordance with the Company's guidelines on Lawful Basis for Processing Personal Data.

5.2. Consent

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

5.2.2. 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.

5.2.3. 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.

5.2.4. 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.

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

5.3. **Transparency (notifying data subjects)**

5.3.1. The UK 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.

5.3.2. 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 UK GDPR including the identity of the Data Controller and DPM, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data..

5.3.3. When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6. Purpose limitation

6.1. 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.

6.2. 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.

7. Data minimisation

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

7.2. 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.

7.3. 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.

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

8. Accuracy

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

8.2. 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.

9. Storage limitation

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

9.2. 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.

10. The Company 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 Company's guidelines on Data Retention.

10.1. 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 Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

10.2. 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.

11. Security integrity and confidentiality

11.1. Protecting Personal Data

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

11.1.2. 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.

11.1.3. 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.

11.1.4. 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.

11.2. You must comply with all applicable aspects of our IT and Information Security Policies (available from IT) and you will not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

11.3. **Reporting a Personal Data Breach**

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

11.3.2. 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.

11.3.3. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPM who will issue a GDPR Incident Report Form. You should preserve all evidence relating to the potential Personal Data Breach.

12. Transfer limitation

12.1. The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK 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.

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

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) 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 DPM;

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

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR 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.

12.3. You must comply with the Company's guidelines on cross border data transfers.

13. Data Subject's rights and requests

13.1. 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.

13.2. 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).

13.3. You must immediately forward any Data Subject request you receive to the DPM and comply with the company's Data Subject response process.

14. Accountability

14.1. 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.

14.2. The Company must have adequate resources and controls in place to ensure and to document UK 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 Company Personnel on the UK 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 Company must maintain a record of training attendance by Company 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.

15. Record keeping

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

15.2. 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 Company's record keeping guidelines.

15.3. These records should include, at a minimum, the name and contact details of the Data Controller and the DPM, 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.

16. Training and audit

16.1. We are required to ensure all Company 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.

16.2. You must undergo all mandatory data privacy related training and ensure your team undergoes similar mandatory training in accordance with the Company's mandatory training guidelines.

16.3. 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.

17. Privacy By Design and Data Protection Impact Assessment (DPIA)

17.1. 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.

17.2. 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 DPM) when implementing major system or business change programs involving the Processing of Personal Data including:

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

(f) Automated Processing including profiling and ADM;

(g) large scale Processing of Sensitive Data; and

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

DPIA must include:

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

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

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

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

17.3. You must comply with the Company's guidelines on DPIA and Privacy by Design.

18. Automated Processing (including profiling) and Automated Decision-Making

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

(a) 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.

18.2. 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.

18.3. 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.

18.4. 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.

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

18.6. Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Company's guidelines on profiling or ADM.

19. Direct marketing

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

19.2. 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.

19.3. 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.

19.4. 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 ensure that marketing preferences are respected in the future.

19.5. You must comply with the Company's guidelines on direct marketing to customers.

20. Sharing Personal Data

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

20.2. You may only share the Personal Data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

20.3. 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 UK GDPR approved third party clauses has been obtained.

20.4. You must comply with the Company's guidelines on sharing data with third parties.

21. Changes to this Data Protection Policy

21.1. We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy.

21.2. This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates. Certain countries may have localised variances to this Data Protection Policy which are available upon request to the DPM.

ends

DATA RETENTION POLICY (UK)

1. ABOUT THIS POLICY

1.1 The corporate information, records and data of Reddo Care & Support CIC is important to how we conduct business and manage employees.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. SCOPE OF POLICY

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage.

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

2.4 This policy applies Reddo Care & Support CIC (and a reference to "**we**", "**us**", "**our**", "**Supplier**", "**Agency**" or "**Reddo**" shall mean the specific company which is delivering services

3. GUIDING PRINCIPLES

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.

- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

4. ROLES AND RESPONSIBILITIES

4.1 **Responsibility of all employees**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Record Retention Schedule, any communications suspending data disposal and any specific instructions from the Legal Department. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 Each of the Reddo companies is responsible for identifying the data that we must or should retain, and determining, in collaboration with the Data Protection Manager (DPM), the proper period of retention. It also arranges for the proper storage and retrieval of data, coordinating with outside vendors where appropriate.

4.3 Each of the Reddo companies is responsible for:

- Administering the data management programme;
- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- Providing guidance, training, monitoring and updating in relation to this policy.

4.4 **Data Protection Manager.** Our Data Protection Manager (DPM) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. Our DPM works with our senior leaders on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Reddo and retained primarily for reference purposes.
- Spam and junk mail.

Please see paragraph 6.2 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 6.3 below for more information on this.

Confidential information belonging to others. Any confidential information that an employee may have obtained from a source outside Reddo, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

6. RETENTION PERIODS

6.1 **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the DPM.

6.2 **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data.

6.4 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information.

However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the DPM.

7. STORAGE, BACK-UP AND DISPOSAL OF DATA

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

7.2 **Destruction**. Each of the Reddo Care & Support CIC group companies is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be coordinated with the IT Department.

7.3 The destruction of data must stop immediately upon notification from the Legal Department that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Legal Department lifts the requirement for preservation.

8. SPECIAL CIRCUMSTANCES

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Record Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Legal Department informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Legal Department determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Legal Department.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

9.1 **Questions about the policy.** Any questions about retention periods relevant to your department should be raised with your department manager. Any questions about this policy should be referred to the DPM, who is in charge of administering, enforcing, and updating this policy.

10. BREACH REPORTING AND AUDIT

10.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depends largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the DPM. If employees do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

10.2 No one will be subject to and we do not allow any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3 **Audits**. Our DPM will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice] to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

ANNEX A DEFINITIONS

Data: all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

Data Protection Manager: our Data Protection Manager is responsible for advising on and monitoring compliance with data protection laws.

Data Retention Policy: this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

Disposable information: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

Personal data: any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health 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, location or date of birth) or an opinion about that person's actions or behaviour.

Record Retention Schedule: the schedule attached to this policy which sets out retention periods for our formal or official records.

Storage limitation principle: data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the UK GDPR as the principle of storage limitation.

ANNEX B RECORD RETENTION SCHEDULE

Establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with the Data Retention Policy.

If you hold data not listed below, please refer to the Data Retention Policy. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact the DPM.

Type	Personal Information To Delete	Retention Period
Worker Seeker	Right to Work & Bank Account information	6 months from registration
Worker Seeker	All information excluding Right to Work & Bank Account information	12 months from registration
Worker (individual who has worked for the company)	All information excluding medical records & pension information	7 years after employment has ceases

Data record types with statutory retention periods

Accident books, accident records/reports
Statutory retention period: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos).
Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

Accounting records
Statutory retention period: 6 years for public limited companies.
Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

Income tax and NI returns, income tax records and correspondence with HMRC
Statutory retention period: not less than 3 years after the end of the financial year to which they relate.

Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

Medical records and details of biological tests under the Control of Lead at Work Regulations Statutory retention period: 40 years from the date of the last entry.
Statutory authority: The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)
Statutory retention period: 40 years from the date of the last entry.
Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates
Statutory retention period: (medical records) 40 years from the date of the last entry; (medical examination certificates) 4 years from the date of issue.
Statutory authority: The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)

Medical records under the Ionising Radiations Regulations 1999
Statutory retention period: until the person reaches 75 years of age, but in any event for at least 50 years.
Statutory authority: The Ionising Radiations Regulations 1999 (SI 1999/3232).

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)
Statutory retention period: 5 years from the date on which the tests were carried out. **Statutory authority:** The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

Records relating to children and young adults
Statutory retention period: until the child/young adult reaches the age of 21.
Statutory authority: Limitation Act 1980.

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity Statutory retention period: 6 years from the end of the scheme year in which the event took place. **Statutory authority:** The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence Statutory retention period: 3 years after the end of the tax year in which the maternity period ends. **Statutory authority:** The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.

Wage/salary records (also overtime, bonuses, expenses) Statutory retention period: 6 years.
Statutory authority: Taxes Management Act 1970.

National minimum wage records
Statutory retention period: 3 years after the end of the pay reference period following the one that the records cover.
Statutory authority: National Minimum Wage Act 1998.

Records relating to working time
Statutory retention period: 2 years from date on which they were made.
Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

Work-seeker records
Statutory retention period: one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.
Statutory authority: The Conduct of Employment Agencies and Employment Businesses Regulations 2003 and The Gangmasters (Licensing Conditions) Rules 2009

Records relating to dealings with other licence holders
Statutory retention period: one year from creation or, where they have been supplied by another person, from last supply.
Statutory authority: The Gangmasters (Licensing Conditions) Rules 2009

Data Record types with non-statutory retention periods Actuarial

valuation reports
Retention period: permanently.

Application forms and interview notes (for unsuccessful candidates) Retention period: One year.

Assessments under health and safety regulations and records of consultations with safety representatives and committees
Retention period: permanently.

Inland Revenue/HMRC approvals
Retention period: permanently.

Money purchase details
Retention period: 6 years after transfer or value taken.

Parental leave
Retention period: 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.

Pension scheme investment policies
Retention period: 12 years from the ending of any benefit payable under the policy.

Pensioners' records
Retention period: 12 years after benefit ceases.

Personnel files and training records (including disciplinary records and working time records) Retention period: 6 years after employment ceases.

Redundancy details, calculations of payments, refunds, notification to the Secretary of State Retention period: 6 years from the date of redundancy

Senior executives' records (that is, those on a senior management team or their equivalents) Retention period: permanently for historical purposes.

Statutory Sick Pay records, calculations, certificates, self-certificates Retention period: The 6 years after the employment ceases.

Trade union agreements
Retention period: 10 years after ceasing to be effective.

Trust deeds and rules Retention period: permanently.

Trustees' minute books Retention period: permanently.

Works council minutes Retention period: permanently.

UK GDPR COMPLIANCE STATEMENT

1. Introduction

1.1. Reddo Care & Support CIC ("we", "our", "us", "the Company", “Reddo”) takes its obligations under UK GDPR and applicable data privacy law seriously. We process Personal Data of our customers, suppliers, employees, workers and other third parties.

1.2. **Scope**

1.3. We recognize that the correct and lawful treatment of Personal Data will maintain confidence in the organization 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.

1.4. The Data Protection Manager (DPM) is responsible for overseeing our Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Georges Debbas, Data Protection Manager, E: office@reddocares.org.uk

1.5. **Personal data protection principles**

We adhere to the principles relating to Processing of Personal Data set out in the UK 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).

STETMENT OF PROCESSING WITH OUR CUSTOMERS

BACKGROUND

The UK GDPR is the UK General Data Protection Regulation. (referred to as "**UK GDPR**" in this document. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK.

UK GDPR is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which came into effect on 25 May 2018 and applied in the UK until 1 January 2021. EU GDPR was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU, it sits alongside and supplements the UK

As a supplier of people-based services, companies in the Reddo Care & Support CIC group act as data controllers for a wide range of personal data as part of the provision of our services, and in receiving such data, our customers are data processors.

In some circumstances, we may also be a data processor for some personal data provided by our customers to us.

In order for Reddo group companies to efficiently continue to deliver services to our customers whilst taking into account the obligations under UK GDPR, it is necessary for us to incorporate a single, consistent, Statement of Processing into our arrangements with our customers, which reflects the manner in which our data may be processed by our customers (and the manner in which we agree to process personal data for which our customers are the data controller).

This Statement of Processing applies Reddo Care & Support CIC (and a reference to "**we**", "**us**", "**our**", "**Supplier**", "**Agency**" or "**Reddo**" shall mean the specific company which is delivering services

"**You**", "**your**", "**yours**", and "**Customer**" means the customer to whom we are delivering services, including any customers within the customer's group.

This Statement of Processing applies to personal data which meets the requirements of applicable Data Protection Legislation (as defined below) which is processed in connection with a Contract (as defined below).

1. APPLICABILITY

1.1. This Statement of Processing applies in the following circumstances:

1.1.1. where we provide services to you or one of your Affiliates;

1.1.2. where we have agreed to undertake any form of data sharing with you or one of your Affiliates;

(and when we refer to the "**Contract**" in this Statement of Processing, we mean the arrangement between us whereby we deliver our services to you in one of the circumstances listed above).

2. COMMENCEMENT AND CONSIDERATION

In consideration of the continued supply of services by us in compliance with UK GDPR (or, in the alternative, in consideration of the sum of £1, receipt of which is duly acknowledged), this Statement of Processing takes effect from 25 May 2018.

This Statement of Processing supersedes any other statements or provisions or contracts or addenda or similar of the Customer which are purported to apply to the Supplier (or in the alternative this Statement of Processing has the effect of terminating and replacing such statements, provisions, addenda or similar).

3. DEFINITIONS AND INTERPRETATION

"Affiliate(s)"	in relation to a body corporate, any subsidiary or holding company of such body corporate, and any subsidiary of any such holding company for the time being.
"Agreed Purpose"	means the provision of personal data from the Supplier to the Customer in order for the Customer to receive the services under the Contract, and where necessary the provision by the Customer of personal data to the Supplier in order for the Supplier to deliver its services under the Contract.
"Contract"	has the meaning given in clause 1.1 above.
"controller", "data controller", "processor", "data processor", "data subject", "personal data", "processing", "sub-processor" and "appropriate technical and organisational measures"	each have the meanings set out in applicable Data Protection Legislation in force at the time.
"Customer's System"	means any IT or web system or computer program or other digital, virtual, or electronic system or service or portal owned or used by the Customer (including where the Customer uses a third party or Managed Services Agent to provide and/or facilitate the same) and into which the Supplier or its sub-processors are required to place Personal Data (or allow Personal Data to be placed), including without limitation any timesheet system, assignment or services tracking system or billing system.

"Reddo Personal Data"	means personal data for which the Supplier is the data controller, and which the Supplier provides to the Customer in order for the Customer to receive the services under the Contract.
"Customer Personal Data"	means personal data for which the Customer is the data controller, and which the Customer provides to the Supplier in order for the Supplier to perform the services under the Contract.
"Data Protection Legislation"	means the **UK General Data Protection Regulation** which came into effect on 1 January 2021 including any national implementing laws, regulations and secondary legislation from such time as it or they may take effect (and as may be amended from time to time).
"Managed Services Agent"	means any company or agency or similar appointed by the Customer in order to manage the receipt of the services under the Contract on the Customer's behalf (and including without limitation any neutral or master vendor, managing agent, or managed services company or other intermediary).
"Permitted Recipients"	mean the parties to the Contract, the employees of each party, any third parties engaged to perform obligations in connection with the Contract (including the auditors of either party) or this Statement of Processing, the professional advisers or representatives or agents (e.g. managed services providers) of each party to the extent that they are required to process the personal data in connection (respectively) the receipt or performance of the services under the Contract.
"Worker" or "Workers"	means any individual used or supplied by the Supplier in order to perform the services under the Contract, including temporary workers (who are under the supervision and control of the Customer) provided by the Supplier when acting as an employment business.

3.1. Unless the context otherwise requires, words in the singular shall include the plural and in the plural include the singular.

3.2. Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

3.3. Any words following the terms **including**, **include**, **in particular**, **for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

3.4. Headings shall be for information only, and shall not be used in order to interpret this Statement of Processing.

3.5. Where the context requires, a reference to legislation, statute, regulation, directive, code which has statutory or legal force (or equivalent) of one country shall be deemed to be a reference to the nearest equivalent legislation, statute, regulation, directive, code which has statutory or legal force (or equivalent) of the country in which the Contract is performed.

3.6. A reference to any legislation, statute, regulation, directive, code which has statutory or legal force (or equivalent) is to that legislation, statute, regulation, directive, code which has statutory or legal force (or equivalent) as it may be amended or updated from time to time.

4. PROCESSING

4.1. Each party shall:

4.1.1. ensure that it has all necessary notices and consents in place to enable lawful transfer of its Personal Data to the Permitted Recipients for the Agreed Purposes;

4.1.2. in respect of Personal Data for which it is the data controller, give full information to any data subject whose personal data may be processed under the Contract of the nature of such processing. This includes giving notice that, on the termination of the Contract, personal data relating to them may be retained by or, as the case may be, transferred to one or more of the Permitted Recipients, their successors and assignees;

4.1.3. process the other's Personal Data only for the Agreed Purposes;

4.1.4. not disclose or allow access to the other's Personal Data to anyone other than the Permitted Recipients;

4.1.5. ensure that all Permitted Recipients are subject to written contractual obligations concerning the other's Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this Statement of Processing; .

4.1.6. not transfer any Personal Data for which it is not the data controller outside the EEA unless the transferor:

4.1.6.1. complies with the provisions of Article 26 of the GDPR (in the event the third party is a joint controller); and

4.1.6.2. ensures that (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 GDPR; or (iii) one of the derogations for specific situations in Article 49 GDPR applies to the transfer.

4.2. Each party shall, to the extent that it is in control of the relevant environment, maintain and shall continue to maintain appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission or communication of data over a network.

5. MUTUAL ASSISTANCE

5.1. Each party shall assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each party shall:

5.1.1. in respect of Personal Data for which it is the data controller, provide to the other upon request copies of any notices given to data subjects in relation to Personal Data it supplies;

5.1.2. promptly inform the other party about the receipt of any data subject access request in respect of Personal Data shared in connection with the Contract;

5.1.3. provide the other party with reasonable assistance in complying with any data subject access request under clause 5.1.2 above;

5.1.4. in respect of Personal Data for which it is the data processor, not disclose or release any Personal Data in response to a data subject access request without first notifying the data controller wherever reasonably practicable;

5.1.5. in respect of Personal Data for which it is the data processor, assist the data controller in responding to any request from a data subject;

5.1.6. provide the data controller with such support as is reasonably required in respect of the Data Protection Legislation's obligations in connection with security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

5.1.7. notify the other party without undue delay on becoming aware of any breach of the Data Protection Legislation which affects Personal Data for which the other party is the data controller;

5.1.8. at the written direction of the data controller, delete Personal Data of the data controller except to the extent required by law to store the Personal Data, or, where deletion is not feasible or possible, ensure that such Personal Data are made inaccessible (for example in an archived data location where it is not able to be processed);

5.1.9. at the written direction of the data controller, provide Personal Data in an easily readable form in connection with any request by a data subject to port his/her Personal Data, to the extent required and so far as is possible under the Data Protection Legislation;

5.1.10. provide the other party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Legislation, including the procedures to be followed in the event of a data security breach, and dealing with subject access requests or the exercise of other rights by a data subject.

6. APPOINTING SUB-PROCESSORS

6.1. Where it is the data processor, a party shall be permitted to appoint one or more sub-processors and to disclose Personal Data to such sub-processors for processing in connection with the Contract and in accordance with this Statement of Processing provided always that:

6.1.1. the data processor provides the with details of the sub-processor upon request; and

6.1.2. the data processor undertakes appropriate due diligence on each sub-processor to the extent required by Data Protection Legislation; and

6.1.3. the data processor shall remain primarily liable to the data controller for the processing undertaken by its sub-processors;

6.2. The data processor shall use reasonable endeavours to apply the terms of this Statement of Processing (or terms no less onerous) to the processing of the Personal Data by the sub-processor.

7. OBLIGATIONS SPECIFICALLY IN CONNECTION WITH WORKERS' PERSONAL DATA

7.1. The Supplier is the data controller in respect of all Personal Data belonging to its Workers which it supplies to the Customer or Managed Services Agent.

7.2. The Customer and its Managed Services Agent shall not be permitted to process, store, handle, transmit or otherwise use Workers' Personal Data for any purpose other than:

7.2.1. the receipt or performance of the services under the Contract;

7.2.2. the issuance of any security approvals or clearances or identification required under the Contract or required by applicable law; where the Contract is for the provision of temporary or permanent recruitment services, the offering or administration of any assignment or work or employment opportunity for the Workers;

7.2.3. where the Contract is for the provision of cleaning, security, facilities management or technical services, in order to manage and administer attendance at the agreed locations in order to perform the services under the Contract;

7.2.4. where the Contract is for the provision of healthcare services, in order to perform those services in respect of individual service users or Customer employees, and in connection with vetting or safeguarding investigation by relevant law enforcement officials, regulators, safeguarding bodies or statutory bodies (such as the CQC);

7.2.5. in response to a valid and properly documented request by a Government body or authority (or upon an order of a court with appropriate jurisdiction);

7.2.6. In order to comply with applicable local law (in which case the Customer shall notify the Supplier of the legitimate basis under UK GDPR upon which it relies in respect of such processing, so that the Supplier can ensure that data subjects have been properly notified);

7.2.7. in connection with retail sector ethical audits (for retail Customers), or to the extent necessary in order for the Customer to audit the services and/or the charges it has paid (and only where the Contract contains such audit rights for the Customer);

7.2.8. in accordance with any permitted processing specified in the Contract (provided that such permitted processing is in compliance with Data Protection Legislation and the privacy processing notice issued by the Supplier to the Workers).

7.3. Should the Customer wish to undertake any other processing of Workers' Personal Data ("**Customer-Specific Processing**"), the Customer must do so on the basis of

being the data controller for such processing, and must obtain consent (where necessary) or notify the data subject directly of the processing it intends to undertake (including the basis under Data Protection Legislation which it relies in order to undertake such processing). The Supplier shall not be the data controller for Customer-Specific Processing, even if the Supplier agrees to provide any processing notices or declarations or consents to Workers on behalf of the Customer in order to facilitate the Customer-Specific Processing (and in such circumstances, the Supplier acts as the data processor of the Customer).

8. USE OF MANAGED SERVICES AGENT

Where the Customer appoints a Managed Services Agent, the Managed Services Agent is deemed to be the Customer's data processor, and the Customer shall ensure compliance by the Managed Services Provider with all data provisions in this Statement of Processing to the same extent as required for the Customer itself.

9. USE OF PORTALS OR OTHER SYSTEMS, CLOUD SERVICES OR INTERNATIONAL DATA PROCESSING

9.1. The parties agree and acknowledge that the Supplier uses cloud-based services (specifically, Microsoft Outlook for mail and documents, and Amazon Web Services for hosting of some applications and systems) and as such Personal Data provided to the Supplier may be held or transmitted or processed on servers owned or operated by the cloud-services provider which may from time to time be located outside the EEA. The Supplier has obtained confirmation from cloud-based services providers that they and their services comply with UK GDPR.

9.2. The Supplier's support functions (such as legal, accounting and finance, payroll, HR and senior management) may be delivered by staff employed or engaged in a different legal entity from the Reddo Care & Support CIC group company which is a party to the Contract. The Customer agrees that any Personal Data shared by it under the Contract may be processed by another legal entity within the Reddo group in order for the Supplier to perform the Contract.

9.3. The Supplier uses shared IT systems and platforms, and this means that the Personal Data may be held or processed or stored or accessed in a country which is not the same as the country in which the Supplier itself is located. Save for Personal Data which may be held on an Amazon Web Server or via the One Drive (Microsoft Cloud) (see clause 9.1 above) or which is processed on the Supplier's behalf by a sub-processor, Personal Data within the Supplier's Group which is held on the Supplier's own systems are held in the UK.

9.4. Where the Customer or its Managed Services Agent requires the Supplier to submit any Worker Personal Data into any Customer's System, the Customer remains responsible for ensuring that the Customer's System is adequately secure and safe in accordance with Data Protection Legislation and the Customer confirms that it has taken adequate measures to assess the Customer's System as part of its due diligence when deciding to require the use of the Customer's System for the Workers' Personal Data.

9.5. The Customer confirms that Workers' Personal Data in the Customer's System shall only be processed in accordance with this Statement of Processing.

9.6. The Customer shall ensure that any Personal Data in the Customer's Systems are also included in response to any subject access request under clause 5 of this Statement of Processing.

9.7. Where Personal Data originating in the EEA is Processed by the data processor outside the EEA or in a territory that has not been designated by the European Commission as ensuring an adequate level of protection pursuant to Data Protection Legislation, the parties agree that the transfer will be subject to any transfer contract clauses as the supervisory authorities may from time to time define, unless the party undertaking the transfer has determined through other valid means that the transfer complies with the Data Protection Legislation.

10. INCORPORATION OF STANDARD CLAUSES

The parties agree that if the Data Protection Legislation or the relevant supervisory authority provides for data controllers and/or data processors to include mandatory standard contractual clauses in their agreements ("**Standard Clauses**"), the Standard Clauses shall be automatically incorporated into the Contract and this Statement of Processing from the date specified by applicable legislation or by the supervisory authority (as applicable), or such earlier date as the parties may agree in writing. To the extent the Standard Clauses conflict with the Contract or this Statement of Processing, the Standard Clauses shall take precedence.

11. TERMINATION OF STATEMENT OF PROCESSING

This Statement of Processing shall continue for a period of 1 year following the end of the Contract or 1 year following the last performance of the services under the Contract, whichever is the later.

12. PERSONAL DATA BREACH AND NOTIFICATION REQUIREMENTS

12.1. The data processor shall use all reasonable endeavours to notify the data controller no later than within 36 hours after becoming aware of security breaches requiring notification as defined under Data Protection Legislation (a "Security Breach"). Such notification shall, where data processor is in control of the relevant environment, include (i) a detailed description of the Security Breach, (ii) the type of data that was the subject of the Security Breach and (iii) the identity of each affected person (or, where not possible, the approximate number of data subjects and of Personal Data records concerned).

12.2. The data processor shall also advise the data controller of (i) the name and contact details of the data processor's data protection officer or other point of contact where more information can be obtained; (ii) to the extent within its knowledge, a description of the likely consequences of the Security Breach; (iii) where data processor is in control of the relevant environment, a description of the measures taken or proposed to be taken by the data processor to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects; and additionally in such notification or thereafter (iv) as soon as such information can be collected or otherwise becomes available, any other information data controller may reasonably request relating to the Security Breach.

12.3. Where a data processor is in control of the relevant environment, the data processor shall take immediate action to investigate the Security Breach and to identify, prevent and make best efforts to mitigate the effects of any such Security Breach in accordance with its obligations under this clause 12.

12.4. Subject to the data controller's prior agreement, the data processor shall carry out any recovery or other action necessary to remedy the Security Breach.

12.5. The data processor shall not release or publish any filing, communication, notice, press release, or report concerning any Security Breach in respect of Personal Data without the data controller's prior written approval.

13. PRIVACY IMPACT ASSESSMENTS

Where requested to do so by the data controller, the data processor shall assist data controller to carry out a privacy impact assessment of any processing in connection with the services under the Contract, and shall work with data controller in good faith to implement agreed mitigation actions to address privacy or data issues identified as a result of the impact assessment.

14. NOTICES

14.1. Formal written notices to be given under or in connection with this Statement of Processing shall be made in writing in English and shall be deemed to have been duly given: (i) when delivered, if delivered by hand during working hours of the recipient; (ii) if transmitted by email (with no indication of transmission failure or delay, provided a delivery receipt notification is received), 6 hours after the later of the time of sending or the time shown on the delivery receipt notification; and (iii) on the 5th working day following posting, if posted by signed for (postage prepaid) mail or the equivalent in the country of posting.

14.2. The addresses for services shall be:

14.2.1. for the Customer, the Customer's registered address;

14.2.2. for the Supplier, marked for the attention of The Data Protection Manager and sent to Reddo Care & Support CIC 94a Roding Road, IG10 3EF.

14.3. Communications requiring formal written notices may be effected by email, provided that for the Supplier they are sent to office@reddocares.org.uk, and for the Customer they are sent to the main Customer contact used by the Supplier (unless the Customer provides another email address).

14.4. All email requests connected to Personal Data for which the Supplier is either the data controller or the data processor (whether from a data subject, a supervisory authority, government agency or otherwise) must be directed as shown here:

To: office@reddocares.org.uk

Subject line must include: Customer name, Data subject surname and the words "Data Access Request".

15. VARIATION

In order to ensure the continued performance of the services under the Contract in compliance with Data Protection Legislation, this Statement of Processing may be varied by the Supplier from time to time upon written notice.

16. SEVERABILITY

If a court of competent jurisdiction declares any provision of this Statement of Processing to be invalid, unlawful or unenforceable as drafted, the parties intend that such provision be amended and construed in a manner designed to give effect to the purposes of the provision to the fullest extent permitted by applicable law. If such provision cannot be so

amended and construed, it shall be severed, and the remaining provisions shall remain unimpaired and in full force and effect to the fullest extent permitted by applicable law.

17. GOVERNING LAW

Notwithstanding any obligations to comply with any local national Data Protection Legislation in the country where the Contract is performed, this Statement of Processing shall be governed by and construed in accordance with the laws of England and Wales, and shall be subject to the exclusive jurisdiction of the English Courts in respect of all Contracts where the Supplier is based in England.

ends

DATA PROCESSING NOTICE
(PROCESSING BY CONSENT)

What is the purpose of this document?

This privacy notice applies to all companies within the Reddo Care & Support CIC group of companies. A reference to "Reddo", "we", "us" or "ours" in this notice is a reference to the specific company in the group which contacts you.

This privacy notice describes how we collect and use personal information about you in connection with marketing activity in accordance with the General Data Protection Regulation and any other applicable privacy laws (referred to as "GDPR" in this notice)

Reddo is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Where can you find a copy of this privacy notice?

A COPY OF THE CURRENT PRIVACY NOTICE IS AVAILABLE ON REQUEST FROM THE DATA PROTECTION MANAGER VIA EMAIL office@reddocares.org.uk

THIS NOTICE MAY BE UPDATED FROM TIME TO TIME.

Data protection principles

We will comply with GDPR. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected for valid purposes that we have clearly explained to you, and not used in a way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about, and limited to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed or made inaccessible (anonymous data or pseudonymised data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

Specific categories of personal data that we could hold about you.

Depending upon your role with us, we will collect, store, and use some or all of the following categories of personal information about you.

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Dates of employment (and dates of assignment).
- Location of employment or workplace.
- Copy of driving licence or details of licence, and details of personal vehicles you use for work (including copies of insurance information).
- Copy of passport (subject to compliance with applicable local law) or information from passport such as passport number together with visas or other records of proof of right to work.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Proof of right to work.

- Details of your timesheets and, if you are an hourly paid frontline operative, details of your assignments.
- Employment records (including job titles, work history, working hours, training records. Qualifications, CVs, job applications, and professional memberships).
- Compensation, commission, expenses and pay history.
- Job or assignment performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information, equipment and communications systems, or our vehicles.
- Photographs might be used for Google+ or ID badges or contact information directories.
- Information connected to compliance with health and safety obligations (such as RIDDOR reports and incident reports).
- Geo location or tracking information connected to performance of your work or assignment.
- IP addresses and device information when you connect to or use our systems or networks.
- Records of (or recordings of) telephone calls, hangouts and meetings.
- Records of drug and alcohol tests.
- Records of competency tests (e.g. language or maths proficiency tests).
- Records of apprenticeship or other training or qualifications undertaken in connection with your employment or engagement via a Reddo company.
- Dietary requirements in the event that you attend a Reddo event.
- Travel booking details.
- Survey responses (such as Candour Surveys which you choose to respond to)
- Social networking posts or messages connected to your job or assignment, or to Reddo.
- Authentication data in connection with our devices or systems.
- Information about you which is connected to claims, legal disputes, legal proceedings or criminal or fraud investigations, or details of IVAs or charging orders (e.g. where a court order requires Reddo to make a deduction from your pay, or pay some of your pay to a third party such as a creditor).
- Financial records information such as credit ratings (for example where a credit check is required as part of your job or assignment).

We may also collect, store and use the following "special categories" of sensitive personal information:officer

- Vetting information relevant to your role (e.g. vetting required by the Security Industry Authority if you are a security officer, or as required if you are working with vulnerable people)
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions (for example in respect of our legal obligations such as Gender Pay Gap reporting, or for diversity monitoring programmes).
- Trades union membership, particularly where we are applying deductions through payroll to a union of your choice.
- Information about your health, including any medical condition, health and sickness records.
- Information about occupational health referrals and outcomes.
- Genetic information and biometric data collected as part of monitoring systems (such as biometric time and attendance systems, biometric security features on company equipment such as laptops).

- Information about criminal convictions and offences to the extent permitted by applicable law (e.g. the Rehabilitation of Offenders Act in the UK).

We will only collect, store and use personal data or special categories of data where this is required in connection with your job or assignment (e.g. to allow us to ensure your wellbeing at work, or in connection with a customer's requirement for a job or assignment).

How is your personal information collected?

We collect personal information through the application, recruitment and onboarding process, either directly from individuals or from an employment agency or umbrella/payroll company or background check provider or through jobs board. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies such as in connection with Disclosure and Barring Services checks.

We will collect additional personal information in the course of your employment or engagement.

We will collect additional information from your use of any "Contact Us" facility on our websites or via any apps we use to facilitate your employment or engagement with us.

If your employment transfers to us under the Transfer of Undertakings (Protection of Employment Regulations 2006 (as amended) or the Acquired Rights Directive or other similar law (referred to collectively as "TUPE"), we will collect information through the TUPE process.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you (this includes offering you work and administering your employment or assignment with us).

2. Where we need to comply with a legal obligation (this includes sharing information with customers and auditors to validate your right to work) for example.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, although these are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

Depending upon your role, we need the types of information in the list above to allow us to perform our contract with you and to enable us to comply with our legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment or employment.

- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the country in which we have employed or engaged you.
- Paying you and, where appropriate, deducting tax and National Insurance contributions.
- Providing benefits to you.
- Liaising with your pension or benefits provider(s).
- Administering the contract we have entered into with you.
- Liaising with customers to whom you are assigned from time to time (including the customer's auditors, professional advisers and compliance teams) regarding your assignment and performance.
- In connection with legal or insurance claims/disputes.
- In connection with health and safety reporting or obligations.
- For business management and planning purposes, including accounting, auditing business sales and restructures.
- When conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications and capability for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- In connection with education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness or other absence.
- To conduct data analytics studies (using anonymised or pseudonymised data) to review and better understand employee retention and attrition rates.
- For equal opportunities monitoring.
- To comply with our legal obligations.
- To prevent or investigate fraud, theft or other wrongdoing.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing you with a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will usually notify you. The exception to this is where the change is

made in respect of one or more categories of employee, worker or contractor (e.g. due to a change in law) in which case such changes will be notified through the publication of a revised privacy notice. We will always endeavour to tell you about these types of changes, and we will explain the legal basis which allows us to undertake this new processing.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection.

We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment (for example in connection with your health, safety, wellbeing, or fitness to work).

3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme].

Less commonly, we may process this type of information where it is needed in relation to legal claims, or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We may use your particularly sensitive personal information in the following ways:

- We may use absence and healthcare information including occupational health information and referrals in connection with absence management or monitoring (including sickness absence, family-related absence or other absence).
- We will use information about your physical or mental health, or disability status to ensure your health, safety and wellbeing in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, and to administer associated benefits.
- We may use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting, or to comply with our legal obligations (such as Gender Pay Gap Reporting).
- We may use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- We may use vetting information relevant to your role (e.g. vetting required by the Security Industry Authority if you are a security officer, or as required if you are working with vulnerable people).

- We may use genetic information and biometric data collected as part of monitoring systems (such as biometric time and attendance systems operated at customer premises, or biometric security features on company equipment such as laptops).
- We will use information about criminal convictions and offences to the extent permitted by applicable law (e.g. the Rehabilitation of Offenders Act in the UK).

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy or to carry out our legal obligations and duties (such as under health & safety legislation) or to exercise specific rights in connection with relevant employment law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. In these limited cases, you should be aware that it is **not** a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the relevant law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- by providing information about unspent convictions to customers who request them in connection with the performance of our services for our customers.
- where required for vetting or validation purposes (such as in connection with security officer roles, or temporary assignments at airports or other ports).
- in connection with safeguarding.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We may use automated job searching through an app or algorithm or, more usually through recruitment jobs boards, which may determine whether your CV is provided in connection with a potential job or application (for example by matching key job titles or phrases against a vacancy).

Except for the job matching referred to above, we do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the Reddo group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, or where it is necessary to administer the working relationship with you, or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes the following types of third-party service providers (including their contractors and designated agents):

1. Customers (where you attend customer premises in connection with your role)
2. Managed services companies or managing agents to whom we provide our services for an end customer.
3. Professional advisers (e.g. lawyers or accountants).
4. Law enforcement or regulatory bodies.
5. The Courts.
6. Insurance companies.
7. Jobs boards and CRM systems (e.g. FileStack, Broadbean, Idibu, Salesforce) used by us or our customers.
8. Benefits providers (e.g. pensions administrators or trustees).
9. CV formatting services providers.
10. Training providers (e.g. in connection with apprenticeships)
11. Payroll or accounting services companies we may use.
12. Auditors (including customer auditors).
13. Providers of apps we use (e.g. Selenity for expenses payments, Docusign for contract signature).
14. Other companies within the Reddo group of companies.
15. Companies that host or provide our IT systems or platforms or apps.
16. Document or data archiving companies we use to store records in line with our legal data retention obligations

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes, unless they obtain permission from you directly to do so. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, through our shared support functions in order to perform our contract with you, and in order to offer you assignments or work elsewhere in the group.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business, with customers to whom you provide services under a contract with us, to umbrella or payroll companies or to companies providing benefits offered to you as part of your employment or engagement with us. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We use cloud-based service providers to host some of our IT systems and apps (including our email and document management systems), and this means that your data may be held outside the EU in those systems. All cloud-based service providers we use have either agreed to specific protections with relevant data authorities, or have agreed to keep personal information in accordance with relevant data protection law.

Data security

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We keep security measures under review and update our procedures and processes as necessary. We limit access to your personal information to those employees and other third parties who have a business need to see it. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise or pseudonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and where possible securely destroy or delete your personal information in accordance with our data retention policy and applicable law.

Where it is not possible to destroy or delete personal information, we may instead move the data to a location which makes it inaccessible. This would have the effect of stopping any processing.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, and in accordance with applicable GDPR or other law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Manager in writing at Reddo Care & Support CIC, 94a Roding Road, IG10 3EF or via email office@reddocares.org.uk.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, unless prevented by law, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In those very limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your

consent, please email office@reddocares.org.uk, making it clear which consent you are seeking to withdraw. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Manager

We have appointed a data protection manager (DPM) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPM office@reddocares.org.uk.

You have the right to make a complaint at any time to the supervisory authority with responsibility for the country in which we have employed or engaged you to work. For further details of the relevant authority, please see these links:

- UK: https://ico.org.uk/

Changes to this privacy notice
We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

ends

DATA PROCESSING NOTICE
(LEGITIMATE BASIS PROCESSING)

What is the purpose of this document?

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation and any other applicable privacy laws (referred to as "GDPR" in this notice).

This notice applies to all employees, workers and contractors engaged or employed or used by us (including permanent salaried colleagues, hourly paid front line operatives, contractors engaged via their own personal services company, and directors).

Reddo is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Where can you find a copy of this privacy notice?

A COPY OF THE CURRENT PRIVACY NOTICE IS ALSO AVAILABLE ON REQUEST FROM THE DATA PROTECTION MANAGER VIA EMAIL office@reddocares.org.uk

THIS PRIVACY NOTICE MAY BE UPDATED FROM TIME TO TIME.

Data protection principles

We will comply with GDPR. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected for valid purposes that we have clearly explained to you, and not used in a way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about, and limited to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed or made inaccessible (anonymous data or pseudonymised data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

Specific categories of personal data that we could hold about you.

Depending upon your role with us, we will collect, store, and use some or all of the following categories of personal information about you.

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Dates of employment (and dates of assignment).
- Location of employment or workplace.
- Copy of driving licence or details of licence, and details of personal vehicles you use for work (including copies of insurance information).
- Copy of passport (subject to compliance with applicable local law) or information from passport such as passport number together with visas or other records of proof of right to work.

- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Proof of right to work.
- Details of your timesheets and, if you are an hourly paid frontline operative, details of your assignments.
- Employment records (including job titles, work history, working hours, training records. Qualifications, CVs, job applications, and professional memberships).
- Compensation, commission, expenses and pay history.
- Job or assignment performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information, equipment and communications systems, or our vehicles.
- Photographs such as these might be used for Google+ or ID badges or contact information directories.
- Information connected to compliance with health and safety obligations (such as RIDDOR reports and incident reports).
- Geo location or tracking information connected to performance of your work or assignment.
- IP addresses and device information when you connect to or use our systems or networks.
- Records of (or recordings of) telephone calls, hangouts and meetings.
- Records of drug and alcohol tests.
- Records of competency tests (e.g. language or maths proficiency tests).
- Records of apprenticeship or other training or qualifications undertaken in connection with your employment or engagement via a Reddo company.
- Dietary requirements in the event that you attend a company event.
- Travel booking details.
- Survey responses (such as Candour Surveys which you choose to respond to)
- Social networking posts or messages connected to your job or assignment, or to Reddo.
- Authentication data in connection with our devices or systems.
- Information about you which is connected to claims, legal disputes, legal proceedings or criminal or fraud investigations, or details of IVAs or charging orders (e.g. where a court order requires Reddo to make a deduction from your pay, or pay some of your pay to a third party such as a creditor).
- Financial records information such as credit ratings (for example where a credit check is required as part of your job or assignment).

We may also collect, store and use the following "special categories" of sensitive personal information:

- Vetting information relevant to your role (e.g. vetting required by the Security Industry Authority if you are a security officer, or as required if you are working with vulnerable people)
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions (for example in respect of our legal obligations such as Gender Pay Gap reporting, or for diversity monitoring programmes).
- Trades union membership, particularly where we are applying deductions through payroll to a union of your choice.
- Information about your health, including any medical condition, health and sickness records.
- Information about occupational health referrals and outcomes.

- Genetic information and biometric data collected as part of monitoring systems (such as biometric time and attendance systems, biometric security features on company equipment such as laptops).
- Information about criminal convictions and offences to the extent permitted by applicable law (e.g. the Rehabilitation of Offenders Act in the UK).

We will only collect, store and use personal data or special categories of data where this is required in connection with your job or assignment (e.g. to allow us to ensure your wellbeing at work, or in connection with a customer's requirement for a job or assignment).

How is your personal information collected?

We collect personal information through the application, recruitment and onboarding process, either directly from individuals or from an employment agency or umbrella/payroll company or background check provider or through jobs board. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies such as in connection with Disclosure and Barring Services checks.

We will collect additional personal information in the course of your employment or engagement.

We will collect additional information from your use of any "Contact Us" facility on our websites or via any apps we use to facilitate your employment or engagement with us.

If your employment transfers to us under the Transfer of Undertakings (Protection of Employment Regulations 2006 (as amended) or the Acquired Rights Directive or other similar law (referred to collectively as "TUPE"), we will collect information through the TUPE process.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you (this includes offering you work and administering your employment or assignment with us).

2. Where we need to comply with a legal obligation (this includes sharing information with customers and auditors to validate your right to work) for example.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, although these are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

Depending upon your role, we need the types of information in the list above to allow us to perform our contract with you and to enable us to comply with our legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment or employment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the country in which we have employed or engaged you.
- Paying you and, where appropriate, deducting tax and National Insurance contributions.
- Providing benefits to you.
- Liaising with your pension or benefits provider(s).
- Administering the contract we have entered into with you.
- Liaising with customers to whom you are assigned from time to time (including the customer's auditors, professional advisers and compliance teams) regarding your assignment and performance.
- In connection with legal or insurance claims/disputes.
- In connection with health and safety reporting or obligations.
- For business management and planning purposes, including accounting, auditing business sales and restructures.
- When conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications and capability for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- In connection with education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness or other absence.
- To conduct data analytics studies (using anonymised or pseudonymised data) to review and better understand employee retention and attrition rates.
- For equal opportunities monitoring.
- To comply with our legal obligations.
- To prevent or investigate fraud, theft or other wrongdoing.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing you with a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will usually notify you. The exception to this is where the change is made in respect of one or more categories of employee, worker or contractor (e.g. due to a change in law) in which case such changes will be notified through the publication of a revised privacy notice. We will always endeavour to tell you about these types of changes, and we will explain the legal basis which allows us to undertake this new processing.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection.

We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment (for example in connection with your health, safety, wellbeing, or fitness to work).

3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme].

Less commonly, we may process this type of information where it is needed in relation to legal claims, or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We may use your particularly sensitive personal information in the following ways:

- We may use absence and healthcare information including occupational health information and referrals in connection with absence management or monitoring (including sickness absence, family-related absence or other absence).
- We will use information about your physical or mental health, or disability status to ensure your health, safety and wellbeing in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, and to administer associated benefits.
- We may use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting, or to comply with our legal obligations (such as Gender Pay Gap Reporting).
- We may use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- We may use vetting information relevant to your role (e.g. vetting required by the Security Industry Authority if you are a security officer, or as required if you are working with vulnerable people).
- We may use genetic information and biometric data collected as part of monitoring systems (such as biometric time and attendance systems operated at customer premises, or biometric security features on company equipment such as laptops).
- We will use information about criminal convictions and offences to the extent permitted by applicable law (e.g. the Rehabilitation of Offenders Act in the UK).

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy or to carry out our legal obligations and duties (such as under health & safety legislation) or to exercise specific rights in connection with relevant employment law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. In these limited cases, you should be aware that it is **not** a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the relevant law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- by providing information about unspent convictions to customers who request them in connection with the performance of our services for our customers.
- where required for vetting or validation purposes (such as in connection with security officer roles, or temporary assignments at airports or other ports).
- in connection with safeguarding.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We may use automated job searching through an app or algorithm or, more usually through recruitment jobs boards, which may determine whether your CV is provided in connection with a potential job or application (for example by matching key job titles or phrases against a vacancy).

Except for the job matching referred to above, we do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the Reddo group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, or where it is necessary to administer the working relationship with you, or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes the following types of third-party service providers (including their contractors and designated agents):

1. Customers (where you attend customer premises in connection with your role)
2. Managed services companies or managing agents to whom we provide our services for an end customer.
3. Professional advisers (e.g. lawyers or accountants).
4. Law enforcement or regulatory bodies.
5. The Courts.
6. Insurance companies.
7. Jobs boards and CRM systems (e.g. FileStack, Broadbean, Idibu, Salesforce) used by us or our customers.
8. Benefits providers (e.g. pensions administrators or trustees).
9. CV formatting services providers.
10. Training providers (e.g. in connection with apprenticeships)
11. Payroll or accounting services companies we may use.
12. Auditors (including customer auditors).
13. Providers of apps we use (e.g. Selenity for expenses payments, Docusign for contract signature).
14. Other companies within the Reddo group.
15. Companies that host or provide our IT systems or platforms or apps.
16. Document or data archiving companies we use to store records in line with our legal data retention obligations

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own

purposes, unless they obtain permission from you directly to do so. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, through our shared support functions in order to perform our contract with you, and in order to offer you assignments or work elsewhere in the group.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business, with customers to whom you provide services under a contract with us, to umbrella or payroll companies or to companies providing benefits offered to you as part of your employment or engagement with us. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We use cloud-based service providers to host some of our IT systems and apps (including our email and document management systems), and this means that your data may be held outside the EU in those systems. All cloud-based service providers we use have either agreed to specific protections with relevant data authorities, or have agreed to keep personal information in accordance with relevant data protection law.

Data security

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We keep security measures under review and update our procedures and processes as necessary. We limit access to your personal information to those employees and other third parties who have a business need to see it. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise or pseudonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and where possible securely destroy or delete your personal information in accordance with our data retention policy and applicable law.

Where it is not possible to destroy or delete personal information, we may instead move the data to a location which makes it inaccessible. This would have the effect of stopping any processing.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, and in accordance with applicable GDPR or other law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Manager in writing at Reddo Care & Support CIC 94a Roding Road, IG10 3EF or via email office@reddocares.org.uk.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, unless prevented by law, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In those very limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please email office@reddocares.org.uk, making it clear which consent you are seeking to withdraw. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Manager

We have appointed a Data Protection Manager (DPM) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPM office@reddocares.org.uk.

You have the right to make a complaint at any time to the supervisory authority with responsibility for the country in which we have employed or engaged you to work. For further details of the relevant authority, please see these links:

- UK: https://ico.org.uk/

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

ends