DATA PROTECTION POLICY

1. About this policy

1.1 In the course of the activities which Siderise Holdings Limited, Siderise Holdings Limited Group, Siderise Limited, and / or its subsidiaries ("Siderise", "we", "our", "us", "company") undertakes, personal data is collected, stored, and processed by us. This personal data belongs to our employees, business contacts at other organisations (including clients and prospective clients), and any other person we come into contact with (including the general public). This personal data is subject to certain legal safeguards specified in the Data Protection Legislation, which imposes restrictions on how organisations may process personal data. For the purposes of this Data Protection Policy (the "Policy"), the Data Protection Legislation includes the EU GDPR, the UK GDPR and the Data Protection Act 2018. Throughout this Policy references to the "GDPR" mean the EU GDPR and the UK GDPR, as applicable ("Data Protection Legislation").

1.2 Siderise recognises that the correct and lawful treatment of personal data will maintain confidence in Siderise and will contribute to successful business operations. Compliance is also a reflection of how the company wants to conduct its business - to protect the rights of employees and other individuals with whom Siderise may deal and to maintain confidence between those with whom it carries out business. It is important that Siderise, as a business, protects all personal data and sensitive personal data.

1.3 Accordingly, the purpose of this Policy is to:

- Better enable Siderise and its employees, contractors, sub-contractors, agents, consultants, partners and other third parties appointed to process personal data on behalf of Siderise to comply with Data Protection Legislation.
- Ensure that all Siderise employees follow good practice in relation to the handling of personal data.
- Protect the rights of Siderise employees and any other individuals which Siderise may deal with.
- Maintain confidence between Siderise and those with whom it carries out business.
- Mitigate the risk of a breach of Data Protection Legislation.

1.4 Compliance with Data Protection Legislation is important, not only because it is a legal requirement, but because it will support and maintain our reputation with our employees and other individuals about whom we collect personal data. Non-compliance with data protection principles can expose Siderise to complaints, regulatory action, fines, and negative publicity.

1.5 This Policy sets out Siderise's organisational procedures for ensuring that personal data collected, used, or stored by us is processed in accordance with relevant legislative requirements and good practice.

1.6 The types of personal data that Siderise may be required to handle include information about current, past, and prospective suppliers, employees, customers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in Data Protection Legislation.

1.7 This Policy and any other documents referred to in it such as the privacy statement are available on our website Home | Siderise and internally the IMS (SharePoint) Business Documents. The privacy statement sets out the basis on which Siderise will process any personal data it collects from data subjects, or that is provided to it by data subjects or other sources.

1.8 All Siderise employees must comply strictly and in good faith with this Policy. Compliance with this Policy is the responsibility of every employee of Siderise, any person who acts on behalf of Siderise, and any person who has responsibilities for the collection, access, or processing of personal data on behalf of Siderise. Contingent workers and third-party consultants, whilst not employees, are also responsible for complying with this Policy. This Policy is not a contractual document and does not form part of any employee's contract of employment. This Policy may therefore be amended by us at any time.

2. Employees who deliberately disregard the procedures and guidelines in this Policy will face disciplinary action.

2.1 Data users within Siderise are obliged to comply with this Policy when processing personal data on behalf of the Company. Any breach of this Policy may result in disciplinary action. Siderise will not hesitate to take legal and/or disciplinary action against those who act in breach of this Policy.

2.2 This Policy sets out guidance and procedures for the employees of Siderise and any person acting on behalf of Siderise, on Data Protection Legislation and its principles.

2.3 Those who engage data processors outside Siderise to process data on behalf of Siderise must ensure that the data processor complies with the terms of a processing agreement with Siderise. A template processing agreement is available by emailing our Data Protection Officer via DPO@siderise.com.

2.4 Breaches of the Data Protection Legislation can result in fines of €20,000,000 or 4% of Siderise's annual turnover, whichever is higher. A data protection breach can also cause very significant reputational damage. In addition, Siderise would have separate liabilities if it were adjudged to have failed to prevent disclosure of data either within the Siderise or by others who are acting on Siderise's behalf.

2.5 All the above underlines why it is important for all Siderise employees and any person, acting on behalf of Siderise, to adhere to this Policy. It contains important obligations. It is designed to address the key dos and don'ts and to set out potential situations that employees could find themselves in and the correct procedures they must follow.

2.6 If any employee suspects that others with whom Siderise does business are disclosing data or processing data unlawfully, they should report this immediately to our Data Protection Officer ("DPO") at DPO@siderise.com. This is an essential obligation for all employees.

2.7 All employees, any person who acts on behalf of Siderise, and any person who has responsibilities for the collection, access, or processing of personal data on behalf of Siderise must ensure that they read this Policy carefully. Contingent workers and third-party consultants, whilst not employees, are also responsible for complying with this Policy. If you have questions or comments about the Policy or require advice in relation to any matters covered in it, please contact DPO@siderise.com.

2.8 The DPO is responsible for ensuring compliance with Data Protection Legislation and with this Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO at DPO@siderise.com.

3. Definitions

3.1 Data controllers are the people who, or organisations which, determine the purposes for which and the manner in which any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. Where a company within Siderise determines the means and purposes for processing personal data, it will be a data controller.

3.2 Data processors include any person or organisation that is not a data user that processes personal data on behalf of Siderise and on the instructions of Siderise. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on Siderise's behalf.

3.3 Data subjects for the purpose of this Policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.4 Data users are those Siderise employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

3.5 The EEA is the European Economic Area. It includes all European Community countries, together with Iceland, Liechtenstein and Norway.

3.6 ePrivacy Regulations (SI 336 of 2011) are a set of rules which are applicable to certain types of data processing, including electronic direct marketing.

3.7 Personal data means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

3.8 Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3.9 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

3.10 Special categories of personal data include information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual orientation, or genetic or biometric data for the purpose of uniquely identifying a natural person.

3.11 The DPO assists Siderise and its employees to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments ("DPIA") and act as a contact point for data subjects and the UK's supervisory authority.

4. Explained: "Personal Data" and "Special Categories of Personal Data"

4.1 Data Protection Legislation imposes restrictions and conditions on how we may process personal data. It also sets out additional restrictions on how we may process special categories of personal data, which is a defined subset of personal data. We look at each of these terms in turn, below.

4.2 Personal data is defined in paragraph 3.7 above; examples of personal data are individual's names, email addresses, dates of birth or IP addresses.

4.3 Special Categories of personal data are defined above in paragraph 3.10. There must be a clear purpose and legal basis for holding this type of data as it is likely to be of a private nature to the data subject. Data Protection Legislation requires that Siderise meet additional conditions before we can process it. In general, we should treat special categories of personal data with greater care, and where relevant, apply more robust security measures to special categories of personal data

than other personal data. Please note that in some circumstances we will treat dietary requirements as being special categories of personal data, for example, where it can identify an individual's religious or other beliefs, or a medical condition.

4.4 For the purposes of Siderise's business, personal data may derive from various sources such as:

- Employees and close relations, e.g., emergency and next of kin contacts
- Ex-employees
- Potential and prospective employees
- Referees
- General public e.g. complaints
- Business contacts at clients (or prospective clients) of Siderise
- Prospect lists
- Details of contacts in supplier trading relationships (personal and contact details of contractors, sub-contractors, suppliers, vendors and agents).

4.5 Each company within Siderise uses a number of IT systems to store and maintain personal data. Each company will be a data controller in respect of its own use of those systems for its own purposes and must ensure that it complies with the Data Protection Legislation in respect of that processing.

5. Data Protection Principles

5.1 There are six principles set down by the GDPR, which are legally binding on Siderise as a data controller. As such, Siderise must ensure that these principles are followed by all Siderise employees who collect, handle or otherwise process personal data on behalf of Siderise.

5.2 Anyone processing personal data must comply with the six enforceable principles of good practice. These provide that the personal data must be: 5.2.1

5.2.1 Processed fairly and lawfully and in a transparent manner in relation to the data subject.

5.2.2 Processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.2.3 Adequate, relevant and not excessive for their purposes.

5.2.4 Accurate and up to date.

5.2.5 Not kept longer than necessary for their purposes.

5.2.6 Processed securely using appropriate technical and organisational measures.

5.3 Data must also:

5.3.1 Be processed in line with data subjects' right

5.3.2 Not be transferred to people or organisations situated in other countries without adequate protection.

6. Fair and Lawful Processing

6.1 Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in Article 6 and 9 of the GDPR. These include, amongst other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6.3 Transparency is key to data protection. Siderise should not mislead or deceive any individual as to the reason for obtaining and using their personal data. They should be given this information ideally at the point of data collection, otherwise, in compliance with the time scales set out in the GDPR. This can be done via privacy statements which Siderise has prepared and issues on its website, or by informing data subjects through telephone calls, emails and letters how we will use their information. Accordingly, the data controller must specify its identity, the reason(s) why the data is being collected and processed, and whether it will be shared with any third party (and anything else the data controller should tell the data subject in the circumstances). We do not need to tell data subjects that we use their information in ways that will be obvious to them: for example, if a business contact gets in touch to ask for further details about the services we offer, it will clearly be within their reasonable expectations that we will use their information to respond to them in relation to their request.

6.4 The processing of the personal data must not be carried out unlawfully, for example in breach of any obligation of confidence and should only be handled in ways that are reasonably expected by data subjects.

7 Processing for Limited Purposes

7.1 In the course of its business, Siderise may collect and process the personal data set out in our privacy statement. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2 We will only process personal data for the specific purposes set out in our privacy statement or for any other purposes permitted by Data Protection Legislation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

8 Notifying Data Subjects

8.1 If we collect personal data directly from data subjects, in accordance with our privacy statements which are held on CRM, we will inform them about:

8.1.1 Our identity and contact details as data controller.

8.1.2 The purpose or purposes and legal basis for which we intend to process that personal data, and the specific legitimate interest relied upon if that is the legal basis for processing.

8.1.3 The types of third parties, if any, with which we will share or to which we will disclose that personal data.

8.1.4 Whether the personal data will be transferred outside the UK and / or EEA and, if so, the safeguards in place.

8.1.5 The period for which their data will be stored, or the criteria used to determine the period of retention.

8.1.6 The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing.

8.1.7 The rights of the data subject to limit processing, request information, request deletion of information or lodge a complaint with the relevant supervisory authority.

8.2 If we receive personal data from a data subject from other sources, we will provide the data subject with the relevant necessary information as soon as possible thereafter.

8.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

9 Adequate, Relevant and Non-Excessive Processing

9.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9.2 Siderise would be in breach of this principle were it to hold personal data for no specific purpose, and simply on the basis that it might be useful in the future.

10 Accurate Data

10.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10.2 It is the responsibility of every Siderise employee who handles personal data to correct inaccuracies in personal data wherever they are noticed or identified, and to keep it up to date, where necessary. You should also ensure that the marketing preferences of relevant individuals are kept up to date. It is not necessary to update historical records.

11 Timely Deletion

11.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11.2 If in doubt as to retention periods generally, please contact the DPO.

12 Processing in Line with Data Subject's Rights

12.1 We will process all personal data in line with data subjects' rights, in particular their right to:

12.1.1 Request access to any data held about them by a data controller.

12.1.2 Prevent the processing of their data for direct-marketing purposes.

12.1.3 Ask to have inaccurate data amended.

12.1.4 Prevent processing that is likely to cause damage or distress to themselves or anyone else.

13 Data Security

13.1 We will process all personal data we hold in accordance with our IT and Security policies or otherwise take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself. Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor.

13.3 We will maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

13.3.1 Confidentiality means that only people who are authorised to use the data can access it.

13.3.2 Integrity means that personal data shall be accurate and suitable for the purpose for which it is processed.

13.3.3 Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on Siderise's central computer system instead of individual PCs.

13.4 Security procedures include:

13.4.1 Entry controls. Any stranger seen in entry-controlled areas should be reported.

13.4.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).

13.4.3 Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

13.4.4 Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13.4.5 In particular, Siderise employees must ensure that:

- Paper files and other records or documents containing personal data (including sensitive personal data) are kept in a secure environment
- Personal data held on computers and computer systems are protected by the use of secure encrypted equipment and/or passwords
- They comply with any relevant password requirements; and
- They report security breaches to the DPO and the Information Security Officer immediately at DPO@siderise.com.

13.5 Siderise employees should also be aware of, and comply with, the ICT policies and procedures.

14 Personal Data Breaches

14.1 Failing to appropriately deal with and report a personal data breach can have serious consequences for Siderise and for data subjects including:

- risk to the data subjects including identity fraud, financial loss, distress or physical harm
- reputational damage to the company
- fines of up to the higher of €20,000,000 or 4% of annual global turnover.

14.2 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A personal data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential personal data breaches are listed below:

- leaving a mobile device on a train
- theft of a bag containing paper documents
- destruction of the only copy of a document; and
- sending an email or attachment to the wrong recipient.

Reporting a Personal Data Breach

14.3 If you suspect a personal data breach may have occurred then you must contact the DPO immediately at: @DPO@siderise.com

14.4 If a supervisory authority has to be notified by law in relation to the personal data breach, then notification must be made within 72 hours of discovery of the breach where we are a data controller of the compromised data. We may also be contractually required to notify a data controller of the breach immediately upon discovery. It is therefore important that all potential personal data breaches are reported internally to the Data Protection Compliance Manager immediately. Staff who fail to report a potential personal data breach could face disciplinary action.

Investigating a Personal Data Breach

14.5 The DPO will assess and investigate each report of a potential personal data breach and take steps to mitigate the effects of the personal data breach, assess the extent of the personal data breach and consider whether the notification to the supervisory authority or a data subject is required. You should not contact the affected data subject yourself in the event that you have caused a personal data breach.

External communication

14.6 This includes all communications to Law Enforcement, including the Police, other data controllers, supervisory authorities, the Press, and data subjects.

15 Transferring Personal Data to a Country Outside the UK / EEA

15.1 We may transfer any personal data we hold to a country outside the UK or EEA or to an international organisation, provided that one of the following conditions applies:

15.1.1 The country to which the personal data is transferred is a country which has been deemed adequate.

15.1.2 The transfer is subject to appropriate safeguards set out in Data Protection Legislation, including use of the approved model clauses.

15.1.3 The company we transfer data to is signed up to appropriate certification.

15.1.4 The transfer occurs where one or more of the conditions set out in Article 49 GDPR are met.

15.1.5 The transfer is made with the informed consent of the relevant data subject(s).

15.1.6 The transfer is authorised by the relevant supervisory authority where we have adduced adequate safeguards with respect to the protection of the data subject's privacy, their fundamental rights and freedoms, and the exercise of their rights.

15.2 Subject to the requirements in paragraph 15.1 above, personal data we hold may also be processed by staff operating outside the UK / EEA who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15.3 Even if personal data can be lawfully transferred outside the UK / EEA, all of the data protection principles must be adhered to in relation to the relevant personal data.

15.4 If in doubt about transferring personal data generally, please contact the DPO.

16 Disclosure and Sharing of Personal Information

16.1 We may share personal data we hold with any members of the Siderise, which means our subsidiaries, our ultimate holding company, and its subsidiaries, as defined in the relevant sections of the Companies Act 2014 (as amended). Siderise must ensure transfers are subject to appropriate safeguards, and will do so, for example, by corporate governance and where necessary the use of model clauses in intra-company agreements.

16.2 We may also disclose personal data we hold to third parties:

16.2.1 In the event that we sell or buy or receive investment in respect of any business or assets, in which case we may disclose personal data we hold to the prospective seller, buyer or investor of such business or assets.

16.2.2 If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

16.6.3 If we were under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or any other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

16.3 We may also share personal data we hold with selected third parties for the purposes set out in our privacy statement.

16.4 In addition, when transferring any personal data to any Siderise company, you must ensure that:

- You only transfer the minimum amount necessary for the particular purpose of the transfer (for example, a transaction); and
- Adequate security measures are used to protect the personal data during the transfer (including password-protection and encryption).

17 Disclosing Personal Data to Third Parties / Sub-contractors

17.1 As a general rule, only those who have a strict requirement to know personal data will be given access to it. Frequently we wish to share personal data with sub-contractors who are data processors. As a data controller, Siderise remains responsible for their use of such data.

17.2 Accordingly, employees should not disclose any personal data to data processors about former, current, and potential employees, the general public, business contacts of clients, and any other individual about whom we hold personal data, unless the following conditions are met:

17.2.1 You have been specifically authorised to do so by the relevant director of your business area; and

17.2.2 The third party is contractually obliged to:

- Follow Siderise's instructions regarding use of the personal data
- Only use the personal data for Siderise's specified purposes
- Ensure that adequate security measures are used to prevent unauthorised access or damage to the personal data (you should consult the DPO or Information Security Officer about what measures are necessary)
- Notify Siderise immediately in the event of a breach, and provide assistance to us in this eventuality
- Indemnify Siderise in respect of any breach
- Permit Siderise to carry out audits to ensure its compliance with the above.

18 Dealing with Subject Access Requests

18.1 A data subject is entitled to make a formal subject access request ("SAR") for information we hold about them. It is helpful if the person requesting access to their personal data makes the request in writing, identifies the request as a SAR and addresses the request to the DPO. This is not a formal requirement of a SAR. Employees who receive a request that could amount to a SAR should forward it to their line manager or the DPO immediately.

18.2 Employees wishing to make a SAR should do so by emailing Siderise's Data Protection Officer. The Siderise's Data Protection Officer is John McLoughlin, IT Director, Siderise Holdings Limited.

18.3 For more information on how we deal with SARs, please contact the DPO.

19 Disclosing Personal Data to Law Enforcement Agencies

19.1 Pursuant to the transparency requirement, individuals should, as a minimum, be aware that we hold their personal data, why we have it and what it will be used for (see paragraph 8). However, in certain limited circumstances, Data Protection Legislation provides that their personal data (even special categories of personal data) can be shared without their knowledge.

19.2 Data Protection Legislation allows us to share personal data without the data subject being informed of this beforehand in certain cases where to tell the data subject would be likely to prejudice:

19.2.1 The prevention or detection of crime

19.2.2 The apprehension or prosecution of offenders; and

19.2.3 The assessment or collection of tax or duty.

19.3 For example, telling a business contact that we are sharing their personal data with police to investigate their potential fraud would constitute a tip off and could prejudice the investigation.

19.4 In certain circumstances, Data Protection Legislation also allows us to disclose an individual's personal data where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

19.5 If you receive a request from a court or any regulatory or law enforcement authority for information relating to any person about whom we hold personal data (whether an employee, business contact, or otherwise) you should immediately notify the DPO. No employee may disclose personal data to a court or any such authority unless that disclosure has been authorised by the DPO.

20 Marketing to Individuals

20.1 Siderise may seek to improve its relations with business contacts and its clients (or prospective clients) by keeping them informed of Siderise's services. This will include sending marketing and promotional material to those business contacts via:

20.1.1 Paper-based channels (such as letters); and

20.1.2 Electronic channels (such as emails, fax, social media channels, website, automated calling, and SMS).

20.2 In our commitment to uphold the highest standards of data protection and privacy, Siderise adheres to the ePrivacy Regulations (SI 336 of 2011) for all digital marketing activities. Our practices are designed to respect your privacy and ensure transparency, control, and the protection of your personal data. As a general rule, under these regulations we should not send electronic marketing material to individuals, sole traders, and other organisations (e.g., certain types of partnerships) without first obtaining their consent. There is an exception to the requirement to get consent where the 'soft opt-in' applies. That is where the data was obtained in the course of sale or negotiations for sale, only similar products and services are marketed (to the individual who was the subject of the sale, or negotiations for sale) and the individual was given the right to opt out, at the outset and in each subsequent communication.

20.3 When collecting your personal data for marketing purposes Siderise will present a clear and easily understandable consent form that is separate from other terms and conditions. As stated in Recital 32 of the GDPR, silence, pre-ticked boxes, or inactivity will not be considered as validly received data subject consent.

20.4 Siderise may send electronic direct marketing communications to existing customers without explicit consent under specific conditions. These conditions include marketing our own similar products or services that you have previously purchased, provided you were given a clear opportunity to object to such marketing at the time your contact details were collected and in every subsequent communication.

20.5 Based on the current Data Protection Legislation, legitimate interests may be appropriate for 'solicited' marketing (i.e., marketing proactively requested by the relevant person), or for unsolicited marketing in the following circumstances:

20.6 Additionally, no matter what kind of marketing methods or channels we use (i.e., paper-based, or electronic), all marketing communications should allow contacts to opt out of receiving further marketing communications from us, both at the point at which their details are collected, and in each subsequent communication. For example, this could take the form of an 'unsubscribe' link in an email, through a page on the Siderise website or a text short code for SMS messages.

20.7 If any contact states that they do not wish to receive any (or particular) marketing information (about the Siderise's services, for example) then we should comply promptly with this instruction

20.8 If a contact wishes only to receive marketing material from us in a particular way, such as by email or SMS (but not, for example, by letter or telephone), we must ensure that the email marketing system is kept up to date with these particular preferences.

20.9 If a contact wishes only to receive marketing material from us in a particular way, such as by email or SMS (but not, for example, by letter or telephone), we must ensure that the email marketing system is kept up to date with these particular preferences.

20.10 It should be noted that there are more specific rules relating to marketing by facsimile and by means of automated calls in ePrivacy Regulations. Please seek the specific legal advice if you intend to do that.

21 Our Employees

We value the privacy of our employees. This section of the Policy outlines our practices in relation to the collection and use of information about you. Our Employee Privacy Statement can be found on the IMS (SharePoint) Business Documents.

Purpose

21.1 We are aware of our responsibilities as a data controller under Data Protection Legislation and shall endeavour to process any personal data relating to you fairly and lawfully in accordance with Data Protection Legislation.

21.2 We hold and process your personal data for human resources, administration, and management purposes, including:

- Assessment and selection for a position
- Performance reviews
- Training and development
- Payment of pay and benefits
- In relation to pension and other Siderise employee schemes
- Emergency contact(s)
- Health and safety
- Providing references; and
- All other applications of our policies and other terms and conditions of employment.

Collecting Our Employee's Personal Data

21.3 Good employment practice and the efficient running of the business require us to hold certain personal details about you on file. These personal details may include special categories of personal data about you, such as information on your health, racial or ethnic origin or trade union membership. We obtain personal information about you from a number of sources including the application form or CV you submitted when you applied to join, from interview notes and from any details you subsequently provide to us, including on Breathe HR, Sage Payroll and Active Directory], and other IT systems that we use. We will also keep records of, for example, your absence history, your regular performance reviews, in respect of your career development, and any actions or decisions taken as a result of applying any of our policies (in accordance with the terms of the relevant policy). Within Siderise, senior management and HR will have access to your personal information.

21.4 In collecting information about employees or prospective employees, we do not create or use any 'blacklist' of individuals based on their trade union membership or activities or other 'unfair or unlawful grounds' (such as race, ethnic origin etc.). You should always seek advice from the DPO before creating any database of employees or prospective employees.

Using Our Employee's Personal Data

21.5 We will use the personal data we hold about you for purposes connected to your employment.

21.6 As an international organisation, certain personal data will be available within Siderise's offices, or otherwise disclosed to business contacts and other third parties (such as suppliers and business partners), both within and outside the UK / EEA.

21.7 For the purposes set out in this Policy, we may transfer your personal data to third parties (such as insurers, legal, medical and professional advisers, administrators of pension schemes and payroll, and relevant tax authorities, such as HM Revenue & Customs) as permitted by Data Protection Legislation.

21.8 We may also disclose your personal data to other third parties at your own request.

Accuracy

21.9 We will make every effort to ensure that the information held about you is accurate and, where necessary, kept up to date. It is your responsibility to ensure that the information about you contained in our HR database is accurate and kept up to date. You can do this by informing us promptly of any changes to your details, such as a change of address. In the absence of evidence to the contrary we shall assume that the information you provide is accurate. If there is any reasonable doubt as to the accuracy of the data, we shall contact you to confirm the information. Should you inform us, or we otherwise become aware, of any inaccuracies in the information, they shall be rectified promptly.

Retention

21.10 We will retain your Personal Data, in accordance with our Information Retention and Deletion Policy & Schedule. We will not retain information relating to you for longer than is necessary. If information needs to be retained for a longer period, for example, where legal proceedings are involved, the periods will be extended accordingly.

Monitoring of Employee's Communications

21.11 Whilst using Siderise's telephones and IT systems you should have no expectation that your communications will be private. We may monitor electronic communications and record telephone and video conversations by Siderise employees, and their use of websites, for the purpose of ensuring that our IT systems are being used in accordance with Siderise policies and procedures, including with our Siderise Employee Handbook.

21.12 Siderise may monitor your communications for reasons which include: retaining evidence of transactions; ensuring that our procedures, policies and contracts with our employees are adhered to; complying with our legal obligations; monitoring standards of service, employees' performance, and for employees' training; preventing or detecting unauthorised use of our IT systems or criminal activities; and maintaining the effective operation of our IT systems.

21.13 We may use software to monitor and record internet usage. Please bear in mind that you may be called upon to justify the amount of time you have spent on the internet or the sites you have visited. Internet access can be withdrawn from you at any time.

21.14 Telephone, email and internet traffic data may be monitored for the purposes set out above. You should be aware that such monitoring might reveal special categories of personal data about you. For example, if you regularly visit web sites of a particular political party or religious group, then those visits might indicate political opinions or religious beliefs.

21.15 Our processing of any special categories of personal data about you which may be revealed by such monitoring is carried out under legal bases permitted by the Data Protection Legislation.

21.16 In certain circumstances, subject to compliance with any local laws and regulations, emails marked 'PERSONAL' and the content of sites you have looked at or downloaded from the internet may be accessed.

Training

21.17 All employees who have access to any kind of personal data will have their responsibilities under this Policy outlined to them during their induction procedures. We regularly provide our employees with training on data protection issues, and you are required to take part in these sessions when requested by us to do so.

Siderise Employee Handbook

21.18 Other employee policies are described in our Employee Handbook, and you are expected to comply with these policies at all times.

22 Penalties

22.1 Applicable legislation imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this Policy may result in fines being applied.

22.2 Employees also attract personal criminal liability for an unauthorised disclosure or obtaining of personal data. Note also that the breach does not need to be "serious" if it is a marketing breach.

23 Principle Tips: Data Protection Do's and Don'ts

Do's
Do comply with the Data Protection Principles (GDPR) at all times.
Do remember that data protection applies to paper files, electronic information (including all forms of social media), recorded conversations, photographs, videos / DVDs, messaging such as text and instant message, video conferencing and Microsoft Teams communications.
Do ensure that you have a valid lawful basis for processing data. This might involve obtaining consent. Contract the DPO if you are unsure of need support.
Do be extra careful with special category (sensitive) personal data. Follow the guidance in the Siderise policies and procedures and contact the DPO for advice before you process this personal data.
Do keep all personal data secure. Follow the guidance in the Siderise policies and procedures.
Do regularly review all information held and consider if it is appropriate or necessary to delete it; ensure information is kept accurate and up to date.
Do record individual preferences regarding marketing communications and ensure that these databases are updated and shared internally, as necessary, to maintain the accuracy of data held.
Do refer to the other Siderise policies and procedures that connect to data protection, including the Information Retention and Deletion Policy and Schedule, the Privacy Notices, and the Information Security and IT policies.
Do contact the DPO immediately if you think there has been a personal data breach, which includes any loss or suspected loss of data or unauthorised access to data. Report data breaches immediately by contacting DPO@siderise.com.
Do realise that emails and instant messages may be retrieved and revealed to those about whom they are written.
Do contact the DPO if you have any questions about data protection or the GDPR.

Do pass on all Subject Access Requests (SAR) to the DPO as soon as they are received.
Do pass on any correspondence received from any data privacy regulator or courts/other regulatory authorities to the DPO
And finally, BE open and transparent with individuals about how you intend to use their personal data. Refer them to the relevant Privacy Notice when collecting their personal data and as a first port of call for GDPR queries.

Don'ts
DO NOT share personal data with third parties without making sure that you have permission and / or have followed GDPR procedures. Contact the DPO for guidance.
DO NOT hold special category (sensitive) personal data about an individual without a valid lawful basis, which may include the data subject's explicit consent. If you are unsure, contact the DPO for guidance.
DO NOT leave personal data unsecured in any way, whether it this be in the form of physical files or information held electronically.
DO NOT take personal data home without considering its security.
DO NOT transfer personal data outside the UK / EEA unless you have checked with the DPO that there are adequate safeguards in place. This is a requirement of the GDPR.
DO NOT hold personal data about an individual for longer than is necessary for its intended purpose.
DO NOT use personal data obtained and held for one purpose for a different purpose. Check with the DPO if in doubt.
DO NOT send negative comments about any individual via any media, including clients, employees, suppliers, contractors or sub-contractors. If there is an issue which other people need to be aware of, contact your line manager before contacting the person directly.
And finally, TREAT other people's personal data with the same respect you expect to be accorded to your own. If in doubt, ask the DPO for guidance and support.

24 Roles and Responsibilities

24.1 In order for Siderise to carry out its data protection obligations effectively and efficiently in accordance with Data Protection Legislation and this Policy, it is important to ensure that everyone is aware of their respective responsibilities and acts in accordance with them.

24.2 This section sets out the respective responsibilities of the following groups and individuals, who all have a role to play in ensuring data protection compliance at all levels of the business:

- Siderise group
- The DPO
- Siderise Management
- Siderise's employees

24.3 Siderise shall ensure that:

- At all times, there is a nominated DPO with specific responsibility for data protection in the organisation;
- All employees understand that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal data is appropriately trained to do so
- Anyone who wishes to make enquiries about Siderise's handling of personal data, whether an employee, supplier, or a member of the public knows what to do and how to do it
- Queries about Siderise's handling of personal data are dealt with promptly and courteously
- Methods of handling personal data are regularly assessed and evaluated
- Data sharing with third parties is carried out under a written agreement setting out the scope and limits of the sharing
- Any disclosure of personal data to third parties will be in compliance with the procedures outlined in this Policy; and
- A designated DPO will regularly review data protection procedures and guidelines within the organisation.

24.4 The DPO has the responsibility for:

- Briefing the Board on data protection responsibilities and issues
- Reviewing data protection and related policies
- Advising other employees on data protection issues
- Ensuring that data protection training takes place regularly
- Dealing with payments and registrations to the ICO
- Handling SARs and other rights for individuals provided by the GDPR
- Approving unusual or controversial disclosures of personal data
- Approving contracts with data processors
- Handling any personal data losses or breaches, in conjunction with the Board and IT
- The development of best practice guidelines; and
- Carrying out compliance checks throughout the business to ensure adherence to Data Protection Legislation.

24.5 Siderise Management responsibilities:

- Every line manager is responsible for ensuring that their employees operate in compliance with this Policy and have completed the GDPR training;
- Department Heads and Directors are required to consider, and, if necessary, put in place (and document), any additional arrangements within their departments to ensure compliance with the Policy;
- The DPO, is responsible for providing guidance, training, updates, and advice on the Policy; and

- The Siderise Group Chief Executive has overall responsibility for ensuring that Siderise complies with Data Protection Legislation covering the UK and the EEA.

24.6 Siderise employees' responsibilities:

- Compliance with this Policy is the responsibility of every employee of Siderise, any person who acts on behalf of Siderise, and any person who has responsibilities for the collection, access, or processing of personal data on behalf of Siderise. Contingent workers and third-party consultants, whilst not employees, are also responsible for complying with this Policy
- Employees must understand what is meant by "personal data" and "special categories of personal data" and know how to handle such data; and
- Each employee of Siderise is required to:
    - read and understand this Data Protection Policy
    - adhere with and abide by this Data Protection Policy
    - share best practice on data protection issues
    - attend training sessions and read updates as directed
    - read and adhere to any changes or updates to this Data Protection Policy
    - complete and pass the Data Protection E-Learning (online training)
    - report concerns or breaches to the DPO immediately
    - promptly forward any SARs to the DPO
    - promptly forward any correspondence relating to data protection from individuals, or from the ICO or other supervisory authorities, a court, or any regulatory or law enforcement authority, to the DPO.

25 Reporting

25.1 It is the responsibility of every employee who considers that this Policy has not been followed to raise the matter with the DPO immediately.

25.2 Our DPO and Group Board oversees our compliance with Data Protection Legislation and this Policy. Any questions or concerns about the interpretation or operation of this Policy should be directed to the DPO at DPO@siderise.com

26 Policy Breaches

It is a condition of employment that employees abide by the rules and policies issued by Siderise from time to time. In particular, you must follow this Policy at all times when handling personal data. Any breach of this Policy will be taken seriously and may result in disciplinary action. In appropriate cases a breach may be considered to be gross misconduct leading to summary dismissal.

27 Supporting Policies

Employees should also be aware that this Policy has been formulated within the context of, and alongside, the following Siderise policy documents:

28 Policy Communication

28.1 We reserve the right to change this Policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

28.2 It is the responsibility of every employee to ensure they read, comply and keep themselves up to date with all relevant policies.