PRIVACY STANDARD (GDPR VERSION)

1. Interpretation

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.

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: Quod Limited.

Company personnel: All directors, officers, employees, trustees, volunteers, work experience persons, apprentices, workers, contractors, agency workers, consultants, directors and members.

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, signify agreement to the processing of personal data relating to them.

Data controller: The person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. We are a 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 GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to our 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).

General Data Protection Regulation ("***GDPR***"): The General Data Protection Regulation EU 2016/679. Personal data is subject to the legal safeguards specified in the GDPR.

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

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

Privacy by design: Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy guidelines: The Company privacy/GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and related policies, available at BreatheHR.

Privacy notices (AKA 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, privacy notices or a website privacy policy) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.

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

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.

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

2. Introduction

2.1 This Privacy Standard sets out how Quod Limited ("***we***", "***our***", "***us***", "***Quod***", "***the Company***") handles the personal data of our customers, suppliers, employees, workers and other third parties.

2.2 This Privacy Standard 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 Privacy Standard applies to all company personnel ("***you***", "***your***"). You must read, understand

and comply with this Privacy Standard when processing personal data on our behalf and attend any training provided on its requirements. This Privacy Standard sets out what we expect from you, in order for us to comply with applicable law. This Privacy Standard should be interpreted alongside any related policies, training materials or guidelines we may release in order to assist you. Any breach of this Privacy Standard may result in disciplinary action.

2.4 This Privacy Standard (together with related policies and guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

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 the higher of €20 million (approximately £18 million) or 4% of our total worldwide annual turnover for failure to comply with the provisions of the GDPR.

3.2 All Company personnel are responsible for ensuring all Company personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.3 The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing related notices, policies and guidelines. Their contact details are:

The Data Protection Officer
Quod Limited
Ingeni Building
17 Broadwick Street
London
W1F 0DE

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

(a) If you are unsure of the lawful basis, which you are relying on to process personal data (including the legitimate interests used by the Company) (see *Paragraph 5* below).

(b) If you need to rely on consent and/or need to obtain explicit consent (see *Paragraph 5* below).

(c) If you need to draft or amend any Privacy Notices (see *Paragraph 5* below).

(d) If you are unsure about the retention period for the personal data being processed (see *Paragraph 9* below).

(e) If you are unsure about what security or other measures you need to implement to protect personal data (see *Paragraph 10* below).

(f) If there has been a personal data breach (*Paragraph 10* below).

(g) If you are unsure on what basis to transfer personal data outside the EEA (see *Paragraph 11* below).

(h) If you need any assistance in dealing with any rights invoked by a data subject (see *Paragraph 12* below).

(i) Whenever you are engaging in a significant new, or change in, processing activity, which is likely to require a DPIA (see *Paragraph 13* below) 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 (see *Paragraph 13* below).

(k) If you need help complying with applicable law when carrying out direct marketing activities (see *Paragraph 13* below).

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors) (see *Paragraph 13* below).

4. Personal data protection principles

4.1 We adhere to the principles relating to processing of personal data set out in the GDPR, which require personal data to be:

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

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

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

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

(e) Not kept in a form, which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).

(f) Processed in a manner, which 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).

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

5. Lawfulness, fairness, transparency

Lawfulness and fairness

5.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

5.2 We may only collect, process and share personal data fairly and lawfully and for specified purposes. These help ensure that we process personal data fairly and without adversely affecting the data subject.

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

(a) The data subject has given his or her consent.

(b) The processing is necessary for the performance of a contract with the data subject, or in order to take steps (at the request of the data subject) prior to entering into a contract.

(c) To meet our legal obligations.

(d) To protect the data subject's, or another natural person's, vital interests.

(e) To perform a task, which is carried out in the public interest.

(f) To pursue our (or a third party's) legitimate interests (where those interests are not overridden by the interests or fundamental rights and freedoms of the relevant data subject(s) (as per our Privacy Notices and any Fair Processing Notices).

5.4 You must identify the legal ground being relied on for each processing activity.

Consent

5.5 You must identify the legal ground being relied on for each processing activity.

5.6 A Data Controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

5.7 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.

5.8 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Fresh consent may need to be sought if you intend to process personal data for a different and incompatible purpose, which was not disclosed when the data subject first consented.

5.9 The withdrawal of consent does not affect the legality of collection, storage or processing of data, whose lawfulness was based on consent, prior to your withdrawal of consent.

5.10 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 separate Privacy Notice to the data subject, in order to obtain explicit consent.

5.11 You will, subsequently, need to evidence the obtained consent and keep records of all consents, so that the Company can demonstrate compliance with consent requirements.

Transparency (notifying data subjects)

5.12 The GDPR requires us to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

5.13 Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with:

(a) Our identity and contact details, as well as those of our DPO.

(b) The purpose and legal basis (including any legitimate interest we intend to rely upon) for processing the personal data.

(c) The recipients or categories of recipients of the personal data.

(d) Where applicable, the fact that we intend to transfer personal data to countries or international organisations outside the EEA and the existence/absence of an adequacy decision or suitable safeguards.

(e) The retention period for the data, or criteria used to determine that period.

(f) A notification of their right to:

(i) Request access, rectification or erasure of data.

(ii) Restrict processing or object to processing of data.

(iii) Data portability.

(iv) Withdraw consent (where data processing is based upon consent, albeit not affecting the lawfulness of data processing occurring based on consent prior to withdrawal.

(v) Lodge a complaint to a supervisory authority.

(g) A notification as to whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

(h) Meaningful information regarding the existence and logic of any automated decision-making, including profiling. Further, the significance and envisaged consequences of such processing for the data subject.

5.14 This will be achieved via a Privacy Notice, which must be presented when the data subject first provides the personal data.

5.15 When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the data subject with all the above information (excluding (g)) to the data subject, as well as:

(i) The categories of personal data concerned.

(j) Details of from where the data originated and, if applicable, whether it came from publicly accessible sources.

5.16 This information should be provided as soon as possible and, in any event:

(a) Within one month of receiving the personal data.

(b) If the personal data is for the purpose of communication, at the time of the first communication to that data subject.

(c) If a disclosure to another recipient is envisaged, at the latest, when the personal data is first disclosed.

5.17 There are various conditions under which notification should not be sent. Confirmation and advice should be sought from our DPO or a member of our HR team] before sending out such notices.

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 and incompatible purposes from those purposes disclosed when the data 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 our applicable data retention and erasure 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 amend inaccurate or out-of-date personal data, or destroy it in accordance with our guidelines.

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.

9.3 We will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time, taking account of laws, obligations and legitimate interests that may require such data to be kept for a minimum period of time.

9.4 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.

9.5 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 guidelines.

10. Security integrity and confidentiality

Protecting personal data

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

10.2 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. Safeguarding techniques may including use of encryption or pseudonymisation, where appropriate and 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.

10.3 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.

10.4 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.

10.5 You must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

Reporting a personal data breach

10.6 The GDPR requires Data Controllers, such as us, to notify any personal data breach to the applicable regulator and, in certain instances, the data subject.

10.7 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.

10.8 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential personal data breach.

11. Transfer limitation

11.1 The GDPR restricts data transfers to countries outside the EEA, in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country. This includes international organisations which operate outside the EEA, even if they also act within them.

11.2 We are able to transfer data to countries outside the EEA, as well as international organisations in cases where:

(a) The Commission has decided that the country or organisation provides an adequate level of protection.

(b) There is no such decision by the Commission, but appropriate safeguards exist and your rights and effective legal remedies are available (including via binding corporate rules).

(c) There is no Commission decision of adequacy, nor appropriate safeguards (including binding corporate rules), but one of the following applies:

(i) The data subject explicitly consents to the transfer, having been informed of the possible risks.

(ii) The transfer is necessary for the performance of a contract with the data subject, or the implementation of pre-contractual measures taken at their request.

(iii) The transfer is necessary for the conclusion or performance of a contract concluded, in the data subject's interest, between us and another entity.

(iv) The transfer is necessary for important reasons of public interest.

(v) The transfer is necessary for the establishment, exercise or defence of legal claims.

(vi) The transfer is necessary in order to protect your vital interests, or the interests of other persons, where the data subject is physically or legally incapable of giving consent.

(vii) The transfer is made from a register which, according to European Union or national law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, subject to the conditions of European Union or national law.

11.3 If you require any assistance regarding transfers outside the EEA, please contact our DPO.

12. Data subject's rights and requests

12.1 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 where consent was a lawful basis of processing (albeit without it affecting the legality of prior processing).

(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 in specific circumstances, 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 or a third party's 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.

(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.

12.2 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.

12.3 You must immediately forward any request regarding personal data you receive, including data subject requests, to the DPO.

13. Accountability

Compliance

13.1 We, as a 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.

13.2 We must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) Appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy.

(b) Implementing "privacy by design" when processing personal data and completing DPIAs, where processing presents a high risk to rights and freedoms of data subjects.

(c) Integrating data protection into internal documents including this Privacy Standard, related policies, Privacy Notices, etc.

(d) Regularly training company personnel on the GDPR, this Privacy Standard, related policies and 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.

(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.

Record keeping

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

13.4 You must keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

13.5 Where we act as a Data controller, these records should include, as a minimum:

(a) The contact details of Quod, our DPO and any joint controller.

(b) The purposes of the processing.

(c) A description of the categories of data subjects and of the categories of personal data.

(d) The categories of recipients to whom the personal data have been, or will be, disclosed, including recipients outside the EEA or international organisations.

(e) Where applicable, transfers of personal data outside the EEA or to an international organisation, including the identification of that country or international organisation and any documentation of suitable safeguards

(f) Where possible, the envisaged time limits for erasure of the different categories of data.

(g) Where possible, a general description of the technical and organisational security measures in place.

13.6 In the event that we are processing the data ourselves, the records should include, as a minimum:

(a) The contact details of Quod, our DPO and any Data Controller on whose behalf we are processing the data.

(b) The categories of processing carried out.

(c) Where applicable, transfers of personal data outside the EEA or to an international organisation, including the identification of that country or international organisation and any documentation of suitable safeguards.

(d) Where possible, a general description of the technical and organisational security measures in place.

13.7 It is entirely possible, if not the norm, for us to act as both a Data Controller and Data Processor. It is important, therefore, to ensure that the relevant requirements are complied with. Ask your manager or our DPO if you are ever unsure.

Training and audit

13.8 We are required to ensure that 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.

13.9 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

13.10 You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

Privacy by design and data protection impact assessment (DPIA)

13.11 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.

13.12 You must assess what "privacy by design" measures can be implemented on all programs/systems/processes, which 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.

(d) The likelihood and severity of infringement upon the protections, rights and freedoms of data subjects posed by the processing.

(e) The risks of varying the current regime.

13.13 We must also conduct DPIAs in respect to high risk processing.

13.14 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the processing of personal data including:

(a) Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).

(b) Automated processing including profiling and ADM.

(c) Large scale processing of sensitive personal data.

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

13.15 A DPIA must include:

(a) A description of the processing, its purposes and the Data Controller's legitimate interests if appropriate.

(b) An assessment of the necessity and proportionality of the processing in relation to its purpose.

(c) An assessment of the risk to individuals.

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

Automated processing (including profiling) and automated decision-making

13.16 Generally, ADM is prohibited when a decision has a legal or significant effect on an individual unless one of the following applies:

(a) A data subject has explicitly consented.

(b) The processing is authorised by law.

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

13.17 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.

13.18 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.

13.19 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.

13.20 A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken.

Direct marketing

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

13.22 For example, a data subject's prior consent is required for electronic direct marketing (for example, by e-mail, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or e-mails 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.

13.23 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.

13.24 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.

13.25 You must comply with any Company guidelines with respect to direct marketing.

Sharing personal data

13.26 Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

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

13.28 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.

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

14. Changes to this privacy standard

14.1 We reserve the right to change this Privacy Standard at any time, so please check back regularly to obtain the latest copy of this Privacy Standard. We last revised this Privacy Standard on the date set out below. Any summary of key changes document available should be located on BreatheHR.

14.2 This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Company operates.