DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

The electronic version of this document is the latest revision and is a controlled copy. It is the responsibility of the individual to ensure that any paper material is the current revision. The printed version of this Policy is uncontrolled

1. Introduction

1.1. This Policy sets out the obligations of VONEUS LIMITED, a company registered in England and Wales under number 07849963, whose registered office is at The Grange, 100 High Street, London, N14 6BN ("the Company") regarding data subject access requests under the Data Protection Legislation (defined below).

1.2. This Policy also provides guidance on the handling of data subject access requests. The procedures and principles set out herein must always be followed by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Data Protection Officer and Scope of Policy

2.1. The Company's Data Protection Officer is Matthew Appleton, legal-matters@voneus.com. The Data Protection Officer is responsible for administering this Policy; for developing and implementing any applicable related policies (including those referred to in this Policy), procedures, and/or guidelines; for ensuring that all data subject access requests are handled in accordance with the Data Protection Legislation; and for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company have an understanding of the Data Protection Legislation and their obligations under it as it applies to their job role(s). Corruption is the abuse of entrusted power or position for private gain.

2.2. The company collects, holds, and processes personal data and our broadband and telephone customers and employees of the business. The Company is a 'data controller' for the purposes of the Data Protection Legislation.

2.3. Data subjects have rights with respect to their personal data under the Data Protection Legislation. This Policy deals specifically with the right of access (Article 15 of the UK GDPR). Data subjects have the right to find out whether the Company collects, holds, or processes personal data about them, the right to obtain a copy of any such data, and certain other supplementary information. The right of access is designed to help data subjects to understand how and why we use their data, and to check that we are doing so lawfully.

2.4. This Policy is an internal company policy designed to provide guidance on handling data subject access requests. It is not a data protection policy, privacy policy, privacy notice, or similar, and is not designed to be made available to third parties (including, but not limited to, data subjects). This Policy should, where appropriate, be read in conjunction with the Company's Data Protection Policy.

2.5. Any questions relating to this Policy, the Company's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Officer.

2.6. Parts 1 to 4 and Parts 14 to 16 of this Policy apply to all staff and Parts 5 to 13 apply to staff authorised to handle data subject access requests.

3. How to recognise a Data Subject Access Request

3.1. The Data Protection Legislation does not set out a particular format which a data subject access request (hereafter "SAR") must follow. A SAR may be made orally or in writing, to any part of the Company, and by any means of communication. A SAR does not need to use the words 'subject access request', 'data protection', 'personal data' or similar terms, or refer to Article 15 of the UK GDPR (or the EU GDPR). This means that anyone in the Company could receive a SAR and it may not be immediately obvious that a SAR has been received.

3.2. SARs may instead use more general terminology, using terms such as 'information' rather than 'personal data'. For example, a message sent to the Company via social media such as 'please provide details of all the information you have about me' will be a valid SAR and must be treated in the same way as a more formal communication referring specifically to a 'subject access request' and data subjects' rights under the UK GDPR.

3.3. Individuals may make SARs on their own behalf. It is also possible to make an SAR via a third party:

3.3.1. This may be a solicitor making a request on behalf of a client, or it may be one private individual making the request on behalf of another. This is permissible, but you must be satisfied that the individual making the request has the authority to act on behalf of the data subject concerned.

3.3.2. In certain limited cases, an individual may not have the mental capacity to manage their own affairs. In these cases, the Mental Capacity Act 2005 enables a third party to make a SAR on behalf of that individual.

3.3.3. Adults such as parents or guardians, may make SARs on behalf of children. The right of access itself, however, remains the child's right. When dealing with a SAR about a child it is important to consider whether that child is mature enough to understand their rights. If so, a response directly to the child should be considered. It may, however, be permissible to allow the adult to exercise the child's right on the child's behalf if the child has given their authorisation, or if it is evident that doing so is in the child's best interests.

3.4. When a SAR is identified, or if a communication or request is received and you are in anyway unsure whether it is a SAR, it should be immediately forwarded to the Company's Dara Protection Officer as set out below in Part 5.

4. What to do When a Subject Access Request is Received.

4.1. The Company has a limited timeframe within which to respond to a SAR, so it is important to act quickly.

4.2. Unless you are authorised to handle a SAR, it must be forwarded to the Data Protection Officer immediately, as set out in this Part 5. Please do not take any further action with respect to any SAR unless you are authorised to do so.

4.3. SARs may come in any form. This will determine how to forward the SAR to the appropriate member of staff:

4.3.1. For SARs received by email or via social media, the message must be forwarded immediately to the Company's Data Protection Officer.

4.3.2. For SARs received by post or in any other hardcopy form, the SAR should first be scanned and emailed immediately to the Company's Data Protection Officer and the original sent to the same recipient using the most direct and secure means possible (e.g.: in person, by courier if available.

4.3.3. For SARs made verbally, the name and contact details of the data subject should first be recorded before informing the data subject that the Company's Data Protection Officer will contact them for full details of their SAR. The data subject's details, and any other information provided by the data subject should be emailed immediately to the Data Protection Officer, including details of the time and date on which the SAR was made.

4.4. The Company's Data Protection Officer should respond to you, confirming receipt of the SAR, within 3 working days of you sending it. If you do not receive a response within this period, you must contact them again to confirm receipt.

5. Responding to a Subject Access Request Part 1: Identifying Data Subjects and Clarifying Requests

5.1. Before responding to a SAR, all reasonable steps must be taken to verify the identity of the individual making the request and, particularly if the Company is processing a large amount of personal data about them, to clarify their request (i.e., to specify the personal data or processing to which their SAR relates). Information requested for such purposes must be reasonable and proportionate. Individuals must not be asked to provide any more information than is reasonably necessary, nor can a request for clarification be used to narrow the scope of a SAR.

5.2. If additional information is required to confirm an individual's identity, the individual must be informed as soon as possible. If additional information is required, the time limit for responding to a SAR does not begin until that information is received.

5.3. If additional information is required to clarify the SAR, the individual must be informed as soon as possible. If such additional information is required, the time limit for responding to the SAR is paused until a response is received. The time limit is measured in whole days. If, therefore, a response is received on the

same day, the time limit for response is unchanged. (also note the possible extensions to the time limit explained in Part 8, below).

5.4. If a SAR is made by a third party on behalf of a data subject (see Part 4.4), the individual acting on behalf of the data subject must be required to provide sufficient evidence that they are authorised to act on the data subject's behalf.

5.5. Examples of information that may be requested to confirm an individual's identity include (note that formal identity documents should not be requested unless it is necessary to do so):

5.5.1. A copy of the individual's passport;

5.5.2. A copy of the individual's driving licence;

5.5.3. A copy of their broadband or telephony bill;

5.5.4. Verification of current or past employment in the company by virtue of searches in the HR database.

5.6. If, having requested additional information to verify an individual's identity, it is still not possible to do so (if, for example, the individual does not comply), the Company may refuse to comply with a SAR, as set out below in Part 11.

5.7. If, having requested additional information to clarify a SAR, the individual does not comply (e.g. does not respond, or refuses to provide further information), the Company must still endeavour to comply with the SAR by making reasonable searches for the personal data relating to the request. It will also generally be possible to provide some or all the supplementary information required by the Data Protection Legislation (see below in Part 9).

5.8. The Company does not retain personal data for the sole purpose of being able to respond to a potential SAR.

6. Responding to a Subject Access Request Part 2: Fee

6.1. Under normal circumstances, the Data Protection Legislation prohibits the charging of a fee for handling a SAR. The Company does not normally charge for SARs.

6.2. In limited cases, it is permissible to charge a 'reasonable fee' to cover the administrative costs of complying with a SAR if that SAR is 'manifestly unfounded', 'excessive', or if a data subject requests further copies of their data following the SAR. In certain cases, it may also be permissible to refuse to comply with a SAR, as set out in Part 11(b).

6.3. The following factors should be considered when calculating a reasonable fee:

6.3.1. Administrative costs involved in:

6.3.1.1. Assessing whether or not the Company is processing the data subject's information

6.3.1.2. Locating, retrieving, and extracting that information

6.3.1.3. Providing a copy of the information; and

6.3.1.4. Sending the Company's response to the data subject.

6.3.2. Specific costs to be considered include:

6.3.2.1. Photocopying, printing, postage, and any other costs incurred when sending the information to the data subject;

6.3.2.2. Equipment and supplies; and

6.3.2.3. Staff time.

7. Responding to a Subject Access Request Part 3: Time Limits

7.1. Under normal circumstances, the Company must respond to a SAR 'without undue delay' and, at the latest, within one month of receipt . The date of receipt of all SARs must be recorded, along with the due date for response.

7.2. Under the Data Protection Legislation, the one-month period referred to in Part 8.1begins on the calendar day – not business day – that the request is received and ends on the corresponding calendar day in the following month (or, if the following month is shorter and does not have a corresponding day (e.g., January 31st to February 28th), the last day of that month). If the last day of the time limit falls on a weekend or bank holiday, the time limit is extended to the next business day.

7.3. If additional information is required from the individual making the SAR to confirm an individual's identity, as under Part 6.2, the time limit under Part 8.1 begins on the day that such information is received.

7.4. If additional information is required from the individual making the SAR to clarify the SAR, as under part 6.3, the time limit under Part 8.1 is paused until the information is received (unless the response is received on the same day, in which case the time limit is not affected).

7.5. If the SAR is complex, or if the same data subject makes several SARs, it is permissible to extend the time limit by up to two months. If such an extension is necessary, the data subject must be informed, in writing, of the reason(s) for the extension within the original one-month time limit.

8. Responding to a Subject Access Request Part 4: Information to be Provided

8.1. Data subjects must be provided with the following information in response to a SAR:

8.1.1. the purposes of which the Company collects, holds, and processes their personal data;

8.1.2. the categories of personal data involved;

8.1.3. the recipients or categories to whom the Company discloses their personal data;

8.1.4. details of how long the Company retains their personal data or, if there is no fixed period, our criteria for determining how long it will be retained;

8.1.5. details of the data subject's right to ask the Company to rectify or erase their personal data, or to restrict or object to our processing of it;

8.1.6. details of the data subject's right to make a complaint to the ICO;

8.1.7. if any of the personal data in question was not obtained from the data subject, details of the source of that data;

8.1.8. if the Company carries out any automated decision-making (including profiling), details of that automated decision-making, including a meaningful explanation of the logic involved and the significance and envisaged consequences for the data subject (also see Part 9.2); and

8.1.9. if the Company transfers their personal data to a third country or international organisation, details of the safeguards in place to protect that data.

8.2. In cases where a SAR related to automated decision-making, the following shall apply:

8.2.1. Where a SAR relates to the logic underlying an automated decision that has been taken with respect to important matters relating to the data subject, the data subject must be provided with an explanation of the logic involved, subject to the following conditions:

8.2.1.1. the decision-making process in question must be solely automated (i.e. there must be no human involvement in the process); and

8.2.1.2. the information should be provided in such a way as to protect the Company's intellectual property rights and trade secrets.

8.2.2. The data subject may also request information related to the automated decision itself, they may seek to exercise the right to human intervention (i.e. for the Company to appoint a person to review the automated decision), to express their own point of view about the decision, and/or to contest it. If a data subject making a SAR seeks to exercise their rights with respect to automated decisions, the Company's Data Protection Officer shall handle the same in accordance with the Data Protection Legislation.

8.3. The information set out in Parts 9.1 and 9.2 must be provided:

8.3.1. in a concise, transparent, intelligible, and easily accessible form, using clear and plain language;

8.3.2. in writing;

8.3.3. if the data subject has made the SAR electronically, in a commonly used electronic format(unless the data subject requests otherwise); and

8.3.4. where p[possible, by using the Company's SharePoint or Google Drive system, providing secure access for data subjects to their personal data.

8.4. It is important to note that data subjects are only entitled to access personal data that the Company holds about them. If information located in the process of responding to a SAR does not meet the definition of "personal data" (see Part 1), the Data Protection Legislation does not entitle the data subject to access it. In certain cases, it may be necessary to separate personal data from non-personal data when responding to a SAR.

9. Responding to a Subject Access Request Part 5: Locating Information

9.1. The Company holds personal data in the following locations and/or systems. It is important to identify the type(s) of personal data to which a SAR relates in order to search in the correct place:

9.1.1. Customer information: Zoho CRM, Sign and Subscriptions

9.1.2. Analysis platforms: Zoho Analysis

9.1.3. General: SharePoint, OneDrive, Google Workspaces Drive and Exchange e-mail

9.2. The Data Protection Legislation requires the Company to make 'reasonable efforts' to find and retrieve personal data in response to a SAR. The right of access is not limited to that information which is easy to find.

10. Refusing to Respond to a Subject Access Request

10.1. In certain cases, it is permissible for the Company to refuse to comply with a SAR:

10.1.1. if it is not possible to identify the individual making the SAR after requesting additional verification under Part 6.2; or

10.1.2. if the request is 'manifestly unfounded' or 'manifestly excessive', considering a range of factors including (but not limited to) whether the request is repetitive in nature, the nature of the information requested, the context of the request, and the relationship between the Company and the

individual making the request. In such cases, it is also possible to request a 'reasonable fee' to handle it, as set out in Part 7.2.

10.2. If either of the above grounds applies, the Company's refusal to comply with the SAR must be justified and an explanation must be provided to the individual making the SAR within one calendar month after receiving the SAR. The individual must also be informed of their right to complain to the ICO and of the possibility of seeking a judicial remedy.

10.3. Certain exemptions to the right of access are also included in the Data Protection Legislation. Please refer to Part 12 for more information.

11. Exemptions to the Right of Access

11.1. The Data Protection Legislation provides several exemptions which apply to SARs and therefore justify the Company refusing to comply with a SAR. Those most likely to be applicable within the Company are situations in which the personal data in question is:

11.1.1. subject to legal or litigation privilege; or

11.1.2. purely personal or exists for a household activity; or

11.1.3. a reference given (or to be given) in confidence for purposes of employment, training, or education; or

11.1.4. is processed for management forecasting or management planning purposes in relation to a business or other activity (but only to the extent that complying with the SAR would prejudice the conduct of the business or activity); or

11.1.5. consists of records of intentions with respect to negotiations between employer and employee (but only to the extent that complying with the SAR would prejudice such negotiations); or

11.2. Additional exemptions relate to more specific (and generally public) matters such as national security. If any concerns or questions arise with respect to exemptions which may or may not apply during the process of handling a SAR (including, but not limited to those set out above), those questions should be referred to the Company's Data Protection Officer and/or to the ICO.

12. Failure to Comply with this Policy

12.1. Compliance with the Data Protection Legislation is of vital importance to the Company. If we fail to comply with a SAR within the required time limit or fail to provide a data subject with access to the personal data that we hold about them, we will be in breach of our obligations under the Data Protection Legislation.

12.2. Failing to comply with the Data Protection Legislation may put the data subject at risk. It may also result in the following consequences for the Company:

12.2.1. the data subject reporting the Company to the ICO, resulting in an investigation by the ICO;

12.2.2. enforcement action taken against the Company which may result in civil and/or criminal sanctions for the Company and, in certain cases, the individual responsible for the breach;

12.2.3. if the data subject has suffered damage and/or distress because of the Company's breach, the data subject may seek further legal remedies such as damages against the Company; and

12.2.4. a court may order the Company to comply with the SAR in any event if the Company is found to have failed in its compliance with the Data Protection Legislation.

12.3. Failure by any member of staff to comply with this Policy may result in disciplinary action which may include dismissal for gross misconduct.