Individual Rights Guidance (GDPR Compliant)

DATA CONTROLLER: Habasit (UK) Ltd
Habegger House
Gannex Park
Dewsbury Road
Elland
HX5 9AF

1 PURPOSE

1.1 The purpose of this Individual Rights Guidance is to assist Habasit (UK) Ltd (the "**Company**") to recognise and deal with requests made from individuals to exercise their rights under data protection laws, in accordance with its obligations under those laws.

1.2 The Company has a legal obligation to deal with these requests in accordance with the specific procedures, and within the timescales prescribed by law.

1.3 If the Company does not deal with these requests in accordance with the law, then it could be subject to enforcement action from the data privacy regulator, the Information Commissioner's Office (the "**ICO**"), including fines of up to €20,000,000 or 4% of total worldwide annual turnover, whichever is higher, compensation claims from individuals and may suffer significant reputational damage.

1.4 For definitions of capitalised terms used in this guidance, please refer to the Definitions appended at Schedule 1 to this guidance.

2 THE RIGHTS

2.1 The rights which can be exercised against the Company by an individual under the law include:

(a) **The right of subject access** – The right to obtain information about how and why the Company processes personal data about them and to obtain a copy of that data;

(b) **The right to rectification** – The right to require the Company to correct inaccuracies in the personal data held about them and/or to complete any incomplete personal data;

(c) **The right to erasure ("right to be forgotten")** – The right to require the Company to erase their personal data in certain circumstances;

(d) **The right to restriction** – The right to require the Company to restrict its processing of their personal data, under certain circumstances;

(e) **The right to data portability** – The right, in certain circumstances, to obtain a copy of their personal data in a certain format, to allow them to transmit it to another Controller or to require the Company to transmit the data directly to the other Controller; and

(f) **The right to object** - The right to object to the processing of their personal data by the Company under certain circumstances, such as the right to stop the Company processing it for the purposes of direct marketing.

This guidance is divided into Sections dealing with each of the rights set out above with some more generally applicable guidance provided below.

2.2 The law also gives individuals other rights, such as the right not to be subject to a decision based solely on automated processing, but these rights are outside the scope of this guidance. Please speak to the Company's Data Protection Manager for further information.

2.3 Where the Company has appointed a Processor (such as a service provider) to process its personal data, the Company (as the Controller) shall retain responsibility for dealing with individual requests relating to that personal data even if the request is received by the Processor and/or relates to personal data held by the Processor. The Company's standard Data Processor Agreement imposes an obligation on the Processor to assist the Company with responding to individual requests. Where the Processor has entered into the standard Data Processor Agreement (or otherwise agreed to assist the Company with such requests), this obligation should be enforced, where necessary i.e. to obtain information or copies of personal data from the Processor, or to ask them to delete or to correct it.

2.4 Note that the Company cannot extend the one month time limit to respond to a request (explained in Section 3 below), merely because the Company needs to rely on a Processor to provide it with the information the Company needs to respond.

3 TIMING

3.1 The Company has a legal obligation to respond to an individual request confirming that the request has been actioned without undue delay and in any event within **one month** of receipt (subject to limited exceptions explained below).

3.2 **How to apply the time limit in practice**:

For the sake of simplicity, we have decided to apply a 28 day time limit to our response to all individual requests. This time limit should be calculated from the day after the Company receives the request, whether or not the day after is a working day. If the 28th day falls on a weekend or a public holiday, then the Company has until the next working day to respond.

3.3 If the Company decides that it needs proof of identity from a data subject before it actions their request (see Section 4.7 below), (and the Company promptly request it from them), then the time period for actioning the request does not start until the Company receives the proof of identity.

3.4 In some cases, the Company may be permitted to extend the one month time limit for a further two months, namely if the request is complex or the Company has received a number of requests from the data subject (who may be an employee, customer or supplier, for example).

3.5 If the Company believes that it needs to extend the time limit for a response, it must write to the data subject within 28 days of receipt of their request, to inform them of this and give reasons for the delay.

3.6 The ICO's view is that it is unlikely to be reasonable to extend the time limit if:

(a) It is manifestly unfounded or excessive;

(b) An exemption applies; or

(c) The Company is requesting proof of identity before considering the request.

3.7 If you wish to extend the deadline for response to a request, please contact the Company's Data Protection Manager.

3.8 Note that it may take a significant amount of time to respond to and to action a request and so it is important that a request is promptly identified and dealt with effectively. Failure to do to do could result in the consequences set out in Section 1.3 above.

4 RESPONDING TO REQUESTS

4.1 A request does not need to be made using formal language or referring to data protection laws. A request may be made in writing or verbally, or using social media.

4.2 The request can be made to any employee in the Company – the data subject does not need to direct it to a specific point of contact, although the Company will encourage individuals to direct it to its Data Protection Manager. The Company therefore needs to ensure that all employees who may receive a request are trained to identify and deal with a request correctly. Details of each request received should be recorded by the Company's Data Protection Manager, particularly where the request has been made verbally.

4.3 The Company has a legal obligation to respond to all requests in a way that is concise, transparent, intelligible and in an easily accessible form, using clear and plain language. The response should be capable of being understood by the average person. Where a data subject has made a request electronically, the Company should provide its response to the request electronically (and in a commonly used format), where possible, and unless otherwise requested by the data subject.

4.4 **Requests made on behalf of a data subject**:

(a) If a third party makes the request on behalf of the data subject (such as a solicitor acting on their behalf), the Company needs to be satisfied that the third party has authority to act on behalf of the data subject. It is the third party's responsibility to provide evidence of their entitlement, such as a written authority from the data subject or a more general power of attorney.

(b) Where the data subject does not have the mental capacity to manage their own affairs, it is reasonable to assume that any third party who has general authority to manage their property and affairs, has authority to make a request on their behalf.

(c) If the Company thinks that the data subject may not appreciate what information would be disclosed to the third party (for example, when responding to a subject access request), the Company may send the response to the data subject directly. The data subject can then choose

whether to provide the third party with a copy of the data, once they have reviewed it.

4.5 **Fees**:

(a) The Company is not permitted to charge for responding to these requests, unless it has clear grounds to assert that a request is "*manifestly unfounded or excessive, in particular because of their repetitive character*…".[1] Where the Company can assert this, it has the option either to refuse to act on the request or to charge a reasonable fee for the administrative costs of complying with the request.

(b) If the Company decide to charge a fee, the Company should contact the data subject promptly to request the fee and to inform them of the Company's reasons for charging it and of their right to lodge a complaint with the ICO or take legal action. If the Company does this, it does not need to comply with the request until it has received the fee.

4.6 **Refusing to action a request:**

(a) If the Company decides not to comply with a request (on the basis of the criteria described in Section 4.5(a) above or another applicable exemption), it must inform the data subject of this without delay (and at the latest within one month of receipt of the request) including the reasons and it must inform them that they can lodge a complaint with the ICO or take legal action.

(b) The Company must be able to justify its decision when it decides to refuse to action a request and it should maintain clear records of its decision. If the Company is considering not actioning a request or charging for a response, the Data Protection Manager must be consulted.

4.7 **Proof of Identity:**

(a) Where necessary (i.e. where there is any doubt as to the identity of the data subject) the Company should verify the identity of the data subject making the request before actioning it (for example, before providing them with a copy of their personal data). Where possible, this should be done via the Company's existing authentication procedures. However, if this is not possible, then the Company should promptly (not later than 3 days after receipt of the request) request additional information to confirm their identity, informing them why the Company needs it and of their right to make a complaint to the ICO or take legal action;

(b) If the data subject is a current employee, formal verification may not be necessary (i.e. they are emailing using a company email);

(c) If the data subject is a former employee, verification will usually be required;

(d) If verification is required, a passport / driving licence, together with an up to date utility bill is satisfactory.

[1] Article 12(5) of the GDPR

4.8 If you have any questions about how to recognise or deal with a request, please contact your Data Protection Manager.

5 EXEMPTIONS

5.1 In certain restricted circumstances, the Company may be exempt from actioning a request (or part of a request) in accordance with data protection laws. Some information about this is included in the relevant Sections below in this guidance. However, this is a complex legal area, and if you are considering relying on an exemption, or you would like further information about the exemptions which apply, please contact your Data Protection Manager.

6 RIGHT OF DATA SUBJECT ACCESS

6.1 **The Right:**

(a) For the data subject to require the Company to confirm whether or not the Company processes personal data about them and if so, to provide them with the supplementary information set out in Section 6.4 below and to provide them with a copy of their personal data;

(b) This right is designed to help individuals to understand how and why the Company is using their personal data and to check that the Company is using it lawfully.

6.2 **The Request:**

(a) Any request by an individual asking for their own data needs to be treated as a subject access request. They do not need to use the phrase 'subject access request' or refer to data protection laws. A request can be made verbally or in writing.

6.3 **Timing:**

(a) The Company needs to comply with a request without undue delay and in any event within 28 days of receiving the request (unless it is necessary to extend the deadline by up to a further 2 months on the grounds set out in Section 3.4 above);

(b) If the Company needs to request further information to confirm the data subject's identity (see Section 4.7 above) or to clarify the request (see Section 6.10 below), then (as long as the Company requests that information promptly) the period for responding to the request does not start until the Company receives the additional information.

6.4 **The Response – Covering Letter**

(a) The following 'Supplementary Information' must be provided in writing to the data subject:

(i) The purposes of the processing i.e. why does the Company process their personal data?

(ii) The categories of personal data;

(iii) The recipients or categories of recipients to whom the personal data have been, or will be disclosed / shared, including identifying whether a recipient receives personal data outside the EU;

(iv) Where possible, how long the Company thinks it will store the personal data for, or if not, what criteria the Company will use to determine this;

(v) The fact that the data subject has the right to request rectification or erasure of their personal data, the restriction of its processing or to object to the Company's processing of it;

(vi) The right to lodge a complaint to the ICO;

(vii) Where the personal data has not been collected from the data subject themselves, any information the Company has about the source of that personal data (for example, a recruitment agent or a broker);

(viii) Where applicable, the existence of any automated decision-making, including profiling, which produces legal effects concerning them (or similarly significant effects) and at least meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(ix) Where the personal data may be transferred to a country located outside the EU, what safeguards are in place governing this transfer.

This information may be contained in one of the Company's privacy notices.

6.5 The supplementary information should be set out in a covering letter (using the Company's standard template) and sent to the data subject together with a copy of their personal data which the Company holds and/or which the Company's Processors hold on the Company's behalf (subject to the review described in Section 0 below).

6.6 The initial copy must usually be provided free of charge, unless the circumstances in Section 4.5 above apply. A reasonable fee may be charged for further copies.

6.7 **Clear and Intelligible:**

(a) Both the supplementary information provided in the covering letter and the copy of the data attached to it must be capable of being understood by the average person. Explanations should be provided if necessary, for example, to enable the data subject to understand data that is in coded form. However, the Company is not obliged to decipher poor handwriting or to translate data into another language;

(b) If the request has been made electronically, then the Company should provide its response in electronic form (in a commonly used format), unless otherwise requested by the data subject.

6.8 **Reviewing the copy data to be provided to the data subject:**

(a) Unless the request is to provide copies of specific data that are easily retrievable, the Company will need to run searches to find the data subject's personal data to include in the response. It will need to review the resulting documents, emails and other correspondence etc. to determine what personal data it needs to provide to the data subject in its response, including whether any exemptions apply. Further guidance on this process is provided in Sections 6.9 – 6.12 below.

6.9 **Third party personal data:**

(a) Before providing a copy of a document, email etc to the data subject, the Company needs to check through it to ensure that:

(i) The Company is only providing personal data that relates to the data subject themselves and not personal data that relates to third parties. The data subject is only entitled to a copy of personal data that relates to them;

(ii) If third party personal data cannot be separated out from the data subject's personal data, then the third party personal data should be redacted;

(iii) If this is not effective, for example, because the data subject would know the identity of the third party, even if the name is redacted, or because it would render the data subject's personal data unintelligible, then the document or correspondence containing the third party personal data should not be provided to the data subject in the response, unless:

(A) the Company has the consent of the third party to disclose it; or

(B) it is reasonable to disclose that data without their consent.

(b) In deciding whether it is reasonable to disclose the information, the following factors should be taken into account:

(i) The type of information that would be disclosed about the third party;

(ii) Any duty of confidentiality the Company owes to the third party;

(iii) Any steps the Company has taken to seek consent from the third party;

(iv) Whether the third party is capable of giving consent; and

(v) Any express refusal or consent by the third party.

(c) The decision needs to be taken on a 'case-by-case' basis, balancing the requesting data subject's need to receive a copy of the particular data, against the third party's right to privacy. If the third party consents to the

Company disclosing the information about them, then the Company should do so, as it would be considered unreasonable for the Company to withhold it.

6.10 **Large amounts of data:**

(a) If the Company process a large amount of information about the data subject making the request, then when the Company runs the searches, this may result in a substantial volume of emails/documents/correspondence which the Company will need to review, in order to find and provide the data subject's personal data;

(b) Where this is the case, the Company is entitled under data protection laws to ask the data subject to provide more information to clarify their request and to help the Company to narrow down the search results. The Company should only ask for the information that it reasonably needs to do this and the Company should request it as soon as possible. However if the data subject refuses to provide any clarification, the Company must still endeavour to comply with their request by making reasonable searches for the information covered by the request.

6.11 **Refusal:**

(a) If the Company is unwilling or unable to comply with a subject access request (on the grounds set out in Section 6.12), the Company must inform the data subject of this without delay (and at the latest within 28 days of receipt of the request) including the reasons and inform them that they can lodge a complaint with the Company's Data Protection Manager, the ICO or take legal action.

6.12 **Exemptions:**

(a) Data protection laws provide a number of exemptions from the obligation to comply (in full or part) with a subject access request, although they are limited and only apply in certain circumstances;

(b) The Company does not need to disclose any information in response to a subject access request, for example, if:

(i) It is subject to legal professional privilege;

(ii) It would reveal the commission of an offence and therefore expose the individual in question to proceedings for that offence (subject to exceptions);

(iii) It is processed in connection with a corporate finance service, subject to certain conditions;

(iv) It is processed for management forecasting/planning purposes, subject to certain conditions;

(v) It consists of records of the intentions of the Controller in relation to negotiations with the data subject and the disclosure is likely to prejudice those negotiations;

(vi) It consists of a confidential reference given (or to be given) for the purposes of education, training, employment etc.; or

(vii) The Company is required by law to make the personal data available to the public, or to disclose it, or the disclosure is necessary for legal proceedings, or for the purposes of obtaining legal advice or establishing, exercising or defending legal rights and where providing the data in response to a subject access request would prevent the Company from achieving those purposes.

(c) If you are considering relying on an exemption, please promptly contact the Data Protection Manager for advice.

6.13 **Audit:**

(a) A clear audit trail recording any decisions to withhold or provide information in response to a data subject access request or any decision not to comply with it, should be retained. A copy of the request and of the information and data provided to the data subject/withheld should also be retained;

(b) Records will be created, stored and maintained by your Data Protection Manager and retained in accordance with the Company's Records Retention and Destruction Policy.

(c) Subject access requests will be logged, recorded and monitored by the Company's Data Protection Manager.

7 RECTIFICATION

7.1 **The Right:**

(a) For the data subject to require the Company to correct their personal data, if it is inaccurate, or to complete any incomplete personal data, including by means of providing a supplementary statement;

(b) This right has close links with the Company's obligation under data protection laws to ensure that the personal data it keeps is accurate. Even if the Company took steps when the Company obtained the personal data to ensure it was accurate, the Company has an obligation to reconsider the accuracy on request.

7.2 **The Request:**

(a) The request does not need to mention the phrase 'request for rectification' or make any reference to data protection laws. Any challenge by a data subject to the accuracy of their personal data which the Company keep and a request for the Company to correct it, or to take steps to complete data about them which is incomplete, must be treated as a rectification request;

(b) A request can be made in writing or verbally.

7.3 **The Response:**

(a) Verifying the accuracy of the data:

(i) If the Company receives a rectification request, it must take reasonable steps to satisfy itself that the personal data is accurate and to rectify the data if necessary, taking into account the arguments and evidence provided by the data subject;

(ii) Data will be inaccurate if it is misleading as to any matter of fact;

(iii) What steps are reasonable, will depend on the nature of the data and what it is used for. The more important it is to the data subject that the data is accurate, the more effort the Company should put into checking its accuracy. For example, if the data will be used to make significant decisions about the data subject, more effort should be put into verifying its accuracy, than for data that does not have a similar impact. The Company can also take into account any steps the Company has already taken to verify the accuracy of the data, prior to receiving the request;

(iv) If the data in question records an opinion, then it may be difficult to determine whether it is accurate or not, as opinions tend (by their very nature) to be subjective. As long as the record makes it clear that the data is an opinion, and where appropriate, whose opinion it is, this may be sufficient;

(v) Whilst the Company is considering the accuracy of the personal data, it is good practice to restrict its processing of the data, even where the individual has not exercised their right to request a restriction (see Section 9.1(c) below);

(vi) If the Company concludes that the personal data is inaccurate or incomplete, the Company must correct or complete it, and confirm to the data subject that this has been done.

7.4 **Timing:**

(a) The Company must inform the data subject in writing, without undue delay and in any event within 28 days of receipt of their request, (unless it is necessary to extend the deadline up to a further 2 months on the grounds set out in Section 3.4 above), that it has rectified their personal data and/or completed any incomplete data (as requested by the data subject) or that it is satisfied that the data is accurate or complete, and therefore will not be amending the data.

7.5 **Refusal:**

(a) The Company can refuse to comply with the request if it verifies that the personal data is accurate or complete, or if the request is manifestly unfounded or excessive. In certain circumstances, the Company may be able to rely on an exemption from the obligation to rectify the data, provided under data protection laws. For further information, please contact the Data Protection Manager;

(b) If the Company decides not to rectify or to complete the personal data, the Company must inform the data subject of this without delay (and at the latest

within 28 days of receipt of the request) and of the reasons for this and inform them that they can lodge a complaint with the ICO or take legal action.

7.6 **Recipients:**

(a) If the Company has disclosed the personal data to others (including any Processor), it must contact each recipient and inform them of the rectification or completion of the data unless the Company can prove that this would be impossible or would involve disproportionate effort (which is unlikely to apply in most circumstances). The Company must inform the data subject about these recipients if requested.

7.7 **Audit:**

(a) A clear record of the request and any decisions to rectify or complete personal data, or to refuse to do so, along with any recipients who have been informed/or any decision not to inform them (and the reasons) should be retained along with copies of all communications with the data subject.

8 RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN")

8.1 **The Right:**

(a) For the data subject to require the Company to erase personal data about them. The right is not absolute, and only applies where one or more of the following circumstances apply:

(i) The Company no longer needs the personal data for the purposes it collected it;

(ii) The Company relies on the data subject's consent to process the personal data but the data subject has withdrawn that consent and there is no other legal justification under the law to process the personal data;

(iii) The Company relies on the legitimate interests' justification to process the personal data but the data subject objects to the processing of their personal data, and there are no overriding legitimate grounds for the processing;

(iv) The personal data has been processed unlawfully by the Company or a third party; or

(v) The personal data needs to be erased to comply with a legal obligation to which the Company is subject.

(b) **The Request:**

(i) The data subject does not need to use the term 'request for erasure' or 'right to be forgotten' or to refer to data protection laws in order to make a valid request, as long as one of the circumstances in Section 8.1(a) above apply. The request can be made verbally or in writing.

8.2 **Grounds to Refuse to Comply with a Request for Erasure:**

(a) The right to erasure requires a balancing act, between the data subject's right to have the personal data erased and the Company's right to retain it. The Company does not need to erase the personal data if its retention is necessary for one or more of the following purposes:

(i) To exercise the right of freedom of expression and information;

(ii) To comply with an obligation under EU or Member States law to which the Company is subject;

(iii) For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where the erasure of the personal data is likely to render this objective impossible or seriously impair it; or

(iv) For the establishment, exercise or defence of legal claims.

(b) There are also two circumstances where the right to erasure will not apply to Special Category Data:

(i) If the processing is necessary for public health purposes in the public interest; or

(ii) If the processing is necessary for preventative or occupational medicine (i.e. where it is necessary for the working capacity of the employee). This only applies where the data is processed subject to a legal obligation of professional secrecy (such as by a health professional).

8.3 **Refusal:**

(a) The Company can also refuse to comply with a request if it is manifestly unfounded or excessive. In addition, in certain circumstances, the Company may be able to rely on other exemptions from the obligation to erase the data, provided under data protection laws. For further information, please contact the Company's Data Protection Manager.

8.4 **Timing and the Response:**

(a) The Company must inform the data subject in writing, without undue delay and in any event within 28 days of receipt of their request (unless it is necessary to extend the deadline up to a further 2 months on the grounds set out in Section 3.4 above), that it has erased their personal data;

(b) If the Company decides not to erase the personal data, the Company must inform the data subject of this without delay (and at the latest within 28 days of receipt of the request) and of the reasons for this and inform them that they can lodge a complaint with the Company's Data Protection Manager or the ICO or take legal action.

8.5 **Does the Company need to erase personal data from back-up systems?**

(a) If the Company is required to erase the personal data then it will need to take steps to erase it from its back-up systems, as well as live environments. The Company needs to be transparent with the data subject about what will happen to their data when the Company complies with their erasure request, including data held in back-ups;

(b) The Company may be able to erase the data from its live environment immediately, however it may be necessary for the data to remain in the back-up system for a certain period time i.e. until it is overwritten;

(c) Where this is the case, the Company should put the back-up data 'beyond use' which means that the Company must not use it for any other purpose, other than to hold it on the system until it can be overwritten in accordance with an established schedule.

8.6 **Does the Company need to tell other organisations about the erasure of the Personal Data?**

(a) There are two circumstances where the Company will need to tell other organisations about the erasure of a data subject's personal data:

(i) Where the personal data has been disclosed to others – the Company must contact each recipient and inform them of the erasure, unless this is impossible or involves 'disproportionate effort' (which is unlikely to apply in most cases). If asked to, the Company must also inform the data subject about these recipients; or

(ii) Where the personal data has been made public in an online environment (i.e. on a social network, forum or website) - reasonable steps must be taken to inform other Controllers who are processing the data, to erase links to, copies or replication of it. The Company can take into account the available technology and the costs of implementation when determining what steps are 'reasonable'.

8.7 **Audit:**

(a) A clear record of the request and of any decisions taken to erase or refuse to erase personal data (and the measures taken to erase data, including back-ups), and to inform/not to inform recipients or request other Controllers to delete personal data should be retained. This includes the reasons given along with copies of all communications with the data subject and any recipients/ other Controllers.

9 THE RIGHT TO RESTRICTION

9.1 **The Right:**

(a) For the data subject to require the Company to restrict its processing of their personal data. This means that the individual can limit the way in which the

Company uses their data. It is an alternative to asking for the erasure of their data.

(b) This is not an absolute right and only applies in one or more of the following circumstances, where:

(i) The accuracy of the personal data is contested by the data subject. Where this applies, the Company is required to restrict its processing of their personal data for a period enabling the Company to verify the accuracy of the personal data;

(ii) The processing of the personal data is unlawful, but the data subject does not want the Company to erase the personal data, but asks the Company to restrict its use instead;

(iii) The Company no longer needs the personal data for the purposes the Company collected it, but it is required by the data subject to establish, exercise or defend legal claims; or

(iv) The data subject has objected to the processing of their personal data, on the grounds set out in Section 11 (right to object) below, pending verification of whether the Company has any overriding legitimate grounds to retain the personal data.

(c) It is a matter of good practice to automatically restrict the processing of personal data whilst the Company is considering its accuracy or the legitimate grounds for processing it in response to a request by the data subject, even if the Company is not requested to restrict the processing by the data subject.

9.2 **The Request:**

(a) A request does not need to include the term 'request for restriction' or to refer to data protection laws in order to be a valid request, as long as one of the conditions in Section 9.1(b) apply. A request can be made verbally or in writing.

9.3 **The Response and Timing:**

(a) The Company must inform the data subject in writing, without undue delay and in any event within 28 days of receipt of their request (unless it is necessary to extend the deadline up to a further 2 months on the grounds set out in Section 3.4 above), that it has restricted the use of their personal data.

9.4 **Refusal:**

(a) The Company can refuse to comply with a request to restrict the processing of personal data if it is manifestly unfounded or excessive or if another exemption provided under data protection laws applies;

(b) If the Company decides not to restrict the use of the personal data, the Company must inform the data subject of this without delay (and at the latest within 28 days of receipt of the request) including the reasons and inform them that they can lodge a complaint with the Company's Data Protection Manager, the ICO or take legal action. The Data Protection Manager should

be consulted in advance about any decision to refuse to restrict the processing of personal data.

9.5 **What does the Company need to do if it has to restrict the processing of the personal data?**

(a) Whilst a restriction is in place, the Company must not process the personal data in any way, except to store it (and to comply with data protection laws, such as to deal with a data subject's request) unless:

(i) The Company has the data subject's consent;

(ii) It is for the establishment, exercise or defence of legal claims;

(iii) It is for the protection of the rights of another person (natural or legal); or

(iv) It is for reasons of important public interest.

(b) The Company needs processes in place to enable it to restrict personal data when required. This could include:

(i) Temporarily moving the data to another processing system;

(ii) Making the data unavailable to other users; or

(iii) Temporarily removing it from a website.

(c) If the data is processed using an automated filing system, the Company needs to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place; the Company should record a note on the system that the processing of this data has been restricted.

9.6 **Recipients:**

(a) If the Company has disclosed the personal data to others, it must contact each recipient and inform them of the restriction of the personal data unless the Company can prove that this would be impossible or would involve disproportionate effort (which is unlikely to be the case in most circumstances). The Company must inform the data subject about these recipients if requested.

9.7 **When can the Company lift the restriction?**

(a) In most cases, the restriction will not be indefinite, but it will only need to be in place for a certain period of time, such as to enable the Company to verify the accuracy of the personal data or to establish whether it has overriding grounds to continue to process it;

(b) Once the Company has made a decision about the accuracy of the data or the overriding legitimate grounds, it may decide to lift the restriction;

(c) The Company must inform the data subject in writing before it lifts a restriction. If this is on the grounds that the data is accurate or the Company has overriding legitimate grounds, then the Company should also inform the data subject of the reasons for not complying with their request and of their right to make a complaint to the ICO or take legal action.

9.8 **Audit Trail:**

(a) A clear record of the request and of any decisions to restrict the use of personal data (and the measures taken) or to refuse to do so, and of any recipients informed (or which it has decided not to inform), and any decision to lift a restriction should be retained, including the reasons along with copies of all communications with the data subject.

10 THE RIGHT TO DATA PORTABILITY

10.1 **The Right:**

(a) For the data subject to receive their personal data which they have provided to the Company in a 'structured, commonly used and machine-readable format' and if desired the right to have such personal data transmitted directly by the Company to another Controller (where technically feasible) without hindrance;

(b) This right allows individuals to obtain and reuse their personal data for their own purposes across different services. For example, it can enable them to find better deals or understand their energy usage habits;

(c) This right only applies:

(i) Where the lawful basis for the processing of the data by the Company is consent or for the performance of a contract;

(ii) Where the Company is carrying out the processing by automated means (i.e. it does not apply to paper files); and

(iii) To personal data that has been provided by the data subject to the Company as a Controller.

10.2 **What does 'provided to the Company as a Controller' mean?**

(a) This will include personal data that has obviously been provided by the data subject, i.e. a mailing address, username or age. However, it also covers personal data which is drawn from observing the individual's activities, such as:

(i) A history of website usage or search activities;

(ii) Traffic or location data; or

(iii) 'Raw' data processed by connected objects, such as smart meters.

(b) It does not include any additional data that the Company has created based on the data provided to it by the individual. For example, if the Company has

used the data provided to create a 'user profile', the Company would not need to provide that to the individual, although they could obtain a copy of that data via a subject access request.

10.3 **The Request:**

(a) The data subject does not need to mention the term 'right to data portability' or to refer to data protection laws in order to make a valid request, as long as the conditions in Section 10.1(c) apply.

10.4 **Third party data:**

(a) If the requested personal data includes data about others (third party data) then the Company will need to consider whether transmitting the data to the data subject or another Controller would adversely affect that third party's rights. This may not necessarily prevent the Company from complying with the request. However, if the requested data was provided by multiple data subjects (i.e. a joint account) the Company would need to be satisfied that all parties have agreed to the portability request.

10.5 **The Response and Timing:**

(a) The Company must provide the data subject with their personal data in a structured, commonly used and machine-readable format and/or transmit it to another Controller where requested (and write to the data subject to confirm that this has been done), without undue delay and in any event within 28 days of receipt of the request, (unless it is necessary to extend the deadline up to a further 2 months on the grounds set out in Section 3.4 above). Where necessary, the Company should obtain confirmation from the data subject of their instructions, in advance of providing the data;

(b) The data must be securely delivered to the data subject/other Controller, for example, using encryption and/or via strong authentication measures;

(c) The Company can provide the data via a direct transmission of the dataset (or the relevant extracts) or provide an automated tool that allows extraction of the relevant data. The format in which the data is provided should enable re-use of it by the data subject/the other Controller. For example, providing an individual with PDF versions of an email inbox is unlikely to enable it to be easily used. Instead it should be provided in a format that preserves all of the metadata to allow re-use;

(d) Note that compliance with a data portability request does not require the Company to delete the data;

(e) Where the Company is requested by the data subject to transmit the data to another Controller, this must be **"without hindrance",** which means that there should be no legal, technical or financial obstacles which prevent or slow down access, transmission or reuse of the data. For example, requesting payment for delivering the data, lack of interoperability or access to a data format, or excessive delay or complexity in retrieving the full dataset.

10.6 **Refusal:**

(a) The Company can refuse to comply with the request if it is manifestly unfounded or excessive or if another exemption under data protection laws applies;

(b) If the Company decides not to comply with the request, it must inform the data subject of this without delay (and at the latest within 28 days of receipt of the request) including the reasons and inform them that they can lodge a complaint with the ICO or take legal action;

(c) The Company should not refuse to comply with a data portability request on the grounds that the data subject has infringed their contract with the Company, such as where they have an outstanding debt.

10.7 **What about if the Company receives personal data, due to a portability request?**

(a) If personal data is transmitted to us as part of a data portability request, the Company needs to make sure that it processes that data in accordance with data protection laws. This includes ensuring that the Company has a lawful basis to process the data and that it is relevant and not excessive for the purposes for which we will process it. If the Company receives personal data that the Company has no reason to keep, the Company should promptly delete it;

(b) If you have any queries about this, please contact the Company's Data Protection Manager.

10.8 **Audit Trail:**

(a) A clear record of the request and of any decisions to provide personal data to a data subject, to transmit it to another Controller or to refuse to do so, should be kept including the measures taken and copies of any communications with the data subject.

11 RIGHT TO OBJECT

11.1 **The Right:**

(a) For the data subject to object to the processing of their personal data in certain circumstances. Where the objection is to the use of personal data for direct marketing purposes, the right is an absolute right, with no exemptions (see Section 12.2 below);

(b) Otherwise, the right to object is not absolute and can only be exercised in certain circumstances, namely if the processing is for:

(i) The Company's legitimate interests (or those of a third party); or

(ii) A task carried out in the public interest, or the exercise of official authority vested in the Company.

(c) The individual must give specific reasons about why they are objecting to the processing of their personal data, based on their particular situation;

(d) If the Company processes the data for scientific or historical research or statistical purposes, the right to object is more limited.

11.2 **Criteria:**

(a) Where the Company receives an objection, the Company must stop processing the personal data unless:

(i) It can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or

(ii) It needs it in order to establish, exercise or defend legal claims.

(b) In deciding whether the Company has compelling legitimate grounds that override the interests of the individual, the Company will need to balance the individual's rights and freedoms with the Company's legitimate grounds. When doing this the Company should consider the reasons for the objection. If it is made on the grounds that the processing is causing the data subject substantial damage or distress (i.e. if it is causing the data subject financial loss) then the Company should apply more weight to their objection. It is the Company's responsibility to demonstrate that its legitimate grounds override those of the data subject.

11.3 **The Request:**

(a) The data subject does not need to include the phrase 'objection to processing' or refer to data protection laws in order to make a valid request, as long as one of the conditions in Section 11.1(b) apply.

11.4 **The Response and Timing:**

(a) The Company must inform the data subject in writing, without undue delay and in any event within 28 days of receipt of their request, (unless it is necessary to extend the deadline up to a further 2 months on the grounds set out in Section 3.4 above), that it has ceased to process their personal data;

(b) Where the Company is required to comply with a request, the Company will need to stop processing the personal data.

11.5 **Refusal:**

(a) The Company can refuse to comply with the request if it is manifestly unfounded or excessive or if another exemption applies under data protection laws;

(b) If the Company decides not to cease processing the personal data, the Company must inform the data subject of this without delay (and at the latest within 28 days of receipt of the request) including the reasons and inform them that they can lodge a complaint with the Company's Data Protection Manager , the ICO or take legal action.

11.6 **Audit Trail:**

(a) A clear record of the request and of any decisions to comply with an objection (or to refuse to do so) and the measures taken must be retained, including the reasons, along with a copy of any communications with the data subject.

12 RIGHT TO OBJECT TO DIRECT MARKETING

12.1 **The Right:**

(a) For the data subject to stop the Company processing their personal data for direct marketing purposes (including any related profiling).

12.2 **Criteria**

(a) Where the Company receives this type of request from the data subject, the Company must stop using their personal data for direct marketing and related profiling. This does not mean that the Company should erase all of the data subject's personal data from its systems. A record of the objection should be retained on its suppression list to ensure that no further direct marketing is sent to the individual.

(b) All such requests should promptly to be sent to the Customer Care Team via sales.uk@habasit.com or by calling 0333 207 6570.

12.3 **The Response and Timing**

(a) The Company must inform the data subject in writing, without undue delay and in any event within 28 days of receipt of their request, (unless it is necessary to extend the deadline up to a further 2 months on the grounds set out in Section 3.4 above), that it has ceased the use of their personal data for marketing purposes.

12.4 **Audit Trail**

(a) A clear record of the request and when and how the Company stopped processing personal data for marketing/profiling should be retained alongside a copy of any communications with the data subject.