COMMAND POST

Unified Detection Protection & Compliance

Personal Data Privacy Policy

TABLE OF CONTENTS

COMMAND POST PERSONAL DATA PRIVACY POLICY

1. INTRODUCTION

1.1 The <Company> is required to comply with the applicable data privacy laws and regulations in respect of its processing of personal data (such as information about our customers, employees and suppliers). Our objective is to set out the data privacy principles **and** overarching requirements **(as detailed in sections 6 and 7 of**

this Policy) which we will apply to our processing of personal data so that we not only respect the data privacy rights of individuals and process their personal data in accordance with the law, but also safeguard one of our most valuable assets, data

1.2 This Policy is designed to ensure compliance with applicable EU data privacy laws, such as the General Data Protection Regulation (EU) 2016/679 ("GDPR**"), and such standard should ensure compliance in the majority of the jurisdictions in which we operate. Where further measures are needed in particular jurisdictions, the Data Privacy Office will advise impacted stakeholders separately.**

2. YOUR RESPONSIBILITIES

2.1 All employees and contract workers ("Employees**"), must familiarise themselves with this Policy (as well as any other data privacy related policies, procedures and/or processes that may be applicable to your area of work) and comply with them whenever you process personal data. Failure to do so may expose the <Company> to fines and enforcement action taken against it by data protection supervisory authorities, which could result in restrictions being imposed upon the <Company> which prevent us from exploiting personal data commercially and/or to complaints and claims for compensation from affected individuals. There may also be negative publicity as a result of our non- compliance.**

2.2 Any failure to comply with this Policy will be taken seriously, dealt with promptly and may result in disciplinary measures which could ultimately result in dismissal.

3. LEGAL FRAMEWORK

3.1 This Policy has been drafted based on a EU standard which is appropriate for global use and appropriate to businesses of our size, scale, brands and global reach. Even though some of the regulatory standards set out in this Policy may not apply in the jurisdiction where you intend to carry out an activity it is the <Company> policy that you comply with the principles and requirements

set out in this Policy. If you have any queries on this Policy's application or interpretation, please contact the Data Privacy Office.

The <Company> has adopted seven key data privacy principles which must be followed in relation to all processing of personal data, as well as some

overarching requirements. These data privacy principles and requirements are summarised in section 6 of this Policy, with a fuller explanation of what each require set out in section 7 of the Policy.

4. DATA WE PROCESS

4.1 The <Company> processes personal data about a range of Living Persons, such as employees, customers, suppliers and business contacts, and the personal data concerned may be in any form, including but not limited to electronic data, paper documents and disks and all types of processing, whether manual or automated that is under the <Company> possession or control.

4.2 We process personal data for a number of purposes, such as customer administration, marketing, profiling our customers and suppliers, statistical analysis, credit checking, service delivery, employee administration, payroll and employee medical and insurance. It is critical to our business that we are able to use personal data in this way. In order to continue to be able to do so, we must ensure compliance with the principles set out in applicable data privacy laws and regulations and in this Policy.

5. DEFINITIONS

In order to fully appreciate the principles in this Policy it is important for you to understand the meaning of certain key words and phrases. These are set out below:

- Data controller **- is the organisation that determines the purposes for which and the manner in which personal data is processed. For example, <Company> the legal entity is the data controller. Employees are not data controllers. Please note that more than one organisation can be the data controller for the same data.**

- Data processor **- is an organisation appointed by the data controller to process personal data on its behalf. The <Company> appoints external organisations to process personal data on our behalf, on the basis that they follow our instructions and do not make decisions in respect of the processing for their own purposes. Examples of these might include the third party company who performs audits of our call centre performance, our IT outsourced services provider or our customer data analytics provider.**

- Informed Consent **- is any given specific and informed indication of the Living Person's agreement to the processing of his/her personal data.**
- Living Person **- is a living identified, or identifiable individual, about whom we**

process personal data. An identifiable individual is someone who can be identified, directly or indirectly, for example, a person could be identifiable by a name, an identification number, location data or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Under data protection laws and regulations the term 'Data Subject' is used to described a Living Person. However, for ease of reference we have used the term Living Person in this Policy.

- Personal data - **is any information capable of identifying a Living Person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link.**

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

- Processing **- any operation (or set of operations) that is performed upon personal data, whether or not by automatic means, including, but not limited to collection, recording, organisation, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction (and** process**,** processes **and** processed **is interpreted accordingly).**

- Sensitive personal data – **certain types of personal data are considered to be "sensitive" and additional care needs to be taken when handling such data.**

    - **The following personal data is defined by law as sensitive: health; racial or ethnic origin; religious or philosophical opinions; trade union membership; political opinions; sexual life or sexual orientation; genetic or biometric data (for the purpose of uniquely identifying a living individual); criminal history/ criminal convictions.**

    - **Additionally to what is defined by law, the <Company> may require certain other categories of data to be handled with special care.**

References in this Policy to 'we**' and '**our**' refer to the <Company> and '**you**' refers to Employees.**

6. DATA PRIVACY PRINCIPLES

6.1 The <Company> will comply with the following data privacy principles, which promote good conduct in relation to the processing of personal data:

6.1.1 personal data must be processed in a fair, lawful and transparent manner;

6.1.2 personal data must be obtained only for one (or more) specified, explicit and legitimate purpose(s), and must not be further processed in any manner incompatible with that/those purpose(s);

6.1.3 personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;

6.1.4 personal data must be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate (having regard to the purpose(s) for which they are processed) are immediately deleted or rectified;

6.1.5 personal data processed for any purpose(s) must not be kept for longer than is necessary for that/those purpose(s);

6.1.6 appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and

6.1.7 personal data will at all times be processed in a manner that can demonstrate compliance with the above-mentioned data privacy principles.

Please refer to section 7 of this Policy for further details of each of the above-mentioned data privacy principles.

6.2 In addition to the data privacy principles set out above, <Company> will comply with the following overarching requirements:

6.2.1 *Rights of Living Persons* **- personal data must be processed in accordance with the rights of Living Persons under applicable data privacy laws and regulations. These rights may include:**

6.2.1.1 the right of access by the Living Person;

6.2.1.2 the right to rectification of inaccurate personal data;

6.2.1.3 the right to erasure/deletion of personal data, commonly referred to as the "*right to be forgotten***";**

6.2.1.4 the right to restrict processing under certain circumstances;

6.2.1.5 the right to data portability; and

6.2.1.6 the right to object (for example, where personal data are processed for direct marketing purposes) and automated individual decision-making;

6.2.2 *Transferring Personal Data Overseas* **- in general, personal data must only be transferred to a country or territory where (a) the Living Person from which it was originally collected is resident; or (b) the <Company> entity that collected it is established. There are a few exceptions to this general rule which are set out in further detail in sections 8.3 to 8.6 of this Policy;**

6.2.3 *Data Privacy Impact Assessments* **- where a new project or way of working, or proposed changes to an existing project or way of working, involves intensive or higher risk processing of personal data or sensitive personal data, a data privacy impact assessment should be carried out; and**

6.2.4 *Personal Data Breaches* **- all losses of personal data should be contained and remedied as soon as possible and where necessary, all appropriate stakeholders informed of the personal data breach.**

This Policy may be amended from time to time to reflect any changes in laws and regulations. Any queries should be directed to the Data Privacy Office.

7. THE DATA PRIVACY PRINCIPLES EXPLAINED

First principle

Personal data must be processed in a fair, lawful and transparent manner and must not be processed unless (a) at least one of the "conditions" for processing set out below is met; and

(b) in the case of sensitive personal data, further stringent conditions are also met.

This is the first and possibly most important of all the data privacy principles. It requires us to process personal data fairly and lawfully. Each of these requirements is considered in turn below.

Lawful processing

7.1 All processing of personal data must be justified by reference to one of a number of "conditions" for processing. If you cannot find a condition that justifies your processing then the processing may not take place. However, in the majority of cases, processing will be justified on the basis that:

7.1.1 it is in <Company>'s legitimate interests as a business or employer, except where such interests are overridden by the interests or fundamental rights and freedoms of Living Persons;

7.1.2 we have obtained the Living Person's consent to the processing (this is not normally appropriate for Employees);

7.1.3 it is necessary to perform a contract. For example, where an <Company> customer has booked a holiday with <Company> and we process their personal data in order to organise and deliver their holiday; or

7.1.4 it is necessary to comply with a legal obligation to which the <Company> is subject (other than an obligation imposed by contract).

7.2 Sensitive personal data should only be processed where it is absolutely necessary to do so. Additional consideration should be given to the secure storage and transmission of sensitive personal data, and access rights should be strictly limited. In addition, where you are processing data which is classified as sensitive personal data by law, one of the following conditions must be satisfied:

7.2.1 the explicit consent (e.g. by actively ticking a box or making a clear written or oral statement) of the Living Person has been obtained, except where consent is precluded under applicable laws;

7.2.2 the processing is necessary for an obligation of the <Company> under employment law;

7.2.3 the vital interests of the Living Person need to be protected (e.g. in a medical emergency or other life or death situation); or

7.2.4 the processing is necessary for the purpose of legal proceedings or obtaining legal advice.

7.3 If you are considering implementing a new project or way of working or making changes to an existing project or way of working, which will involve the processing of personal data, it is important to consider (and record) the condition which can be relied upon together with the rationale for the processing. <Company> maintains a Personal Data Inventory **which records certain details about all business processes which use personal data. The** Personal Data Inventory **may need to be updated to reflect the new or revised project or way of working.**

7.4 **In addition, in such situations, consideration should be given to whether a** Data Privacy Impact Assessment **should be carried out. Please refer to sections 8.7 to 8.10 of this Policy for further details of data privacy impact assessments and when they should be carried out.**

Fair processing

7.5 The second requirement of the first principle is that personal data must be processed fairly. This means that the way in which personal data is held and used must be kept consistent with the privacy notice provided to the Living Person. We satisfy this requirement in relation to our customers, for example, by informing them in a customer privacy policy, which is made generally available on our website(s), how their personal data is used, (amongst other things) about the types of personal data collected, the purposes for which the personal data are collected, anyone to whom their personal data may be disclosed outside of <Company> and the rights available to them.

7.6 The customer privacy policy must be given to the Living Person at the right time. Where we obtain personal data directly from the Living Person (e.g. as a result of a telephone call or online collection) we must give the customer privacy policy to the Living Person at the time we obtain his data.

7.7 The customer privacy policy must be prominent, in legible font and included at every point where we collect personal data, such as in application forms, websites, call centre scripts, promotion terms and application terms. If, for example, the customer privacy policy is provided online, it must be accessible behind a prominent hypertext link where appropriate in the online journey.

7.8 In certain circumstances, short form privacy notices may be presented to Living Persons and included on data collection forms, internet portals etc., in each case these should include a link to the applicable full privacy policy.

7.9 You can obtain copies of our standard and current customer privacy policies from your line manager or Data Privacy Office. You must not modify any of these customer privacy policies without prior authority. These customer privacy policies have been drafted so that they comply with applicable data privacy laws and regulations and any modification on your part could change that. If you think the customer privacy policies do not cover your particular processing activities you must discuss this in the first instance with your manager.

Second principle

Personal data must be obtained only for one (or more) specified, explicit and legitimate purpose(s), and must not be further processed in any manner incompatible with that/those purpose(s).

7.10 The second data privacy principle sets out two requirements:

7.10.1 personal data must be obtained only for one or more specified and

lawful purposes. Our customer privacy policies will specify the purposes for which we will process personal data and we are not permitted to process those data for a new purpose, without first considering the need to obtain Informed Consent from the Living Person and/or issuing an updated privacy notice; and

7.10.2 personal data must not be further processed in any manner incompatible with the purpose(s) for which the data were originally obtained. A breach of this principle could also result in a breach of the first principle. For example, if a customer privacy policy describes the purposes for which personal data will be used as administration, marketing and risk assessment, we should not use those data for any other purposes, unless those additional purposes would be totally obvious to the individual. To do otherwise could result in unfair processing in breach of the first principle and a breach of the second principle.

Third principle

Personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

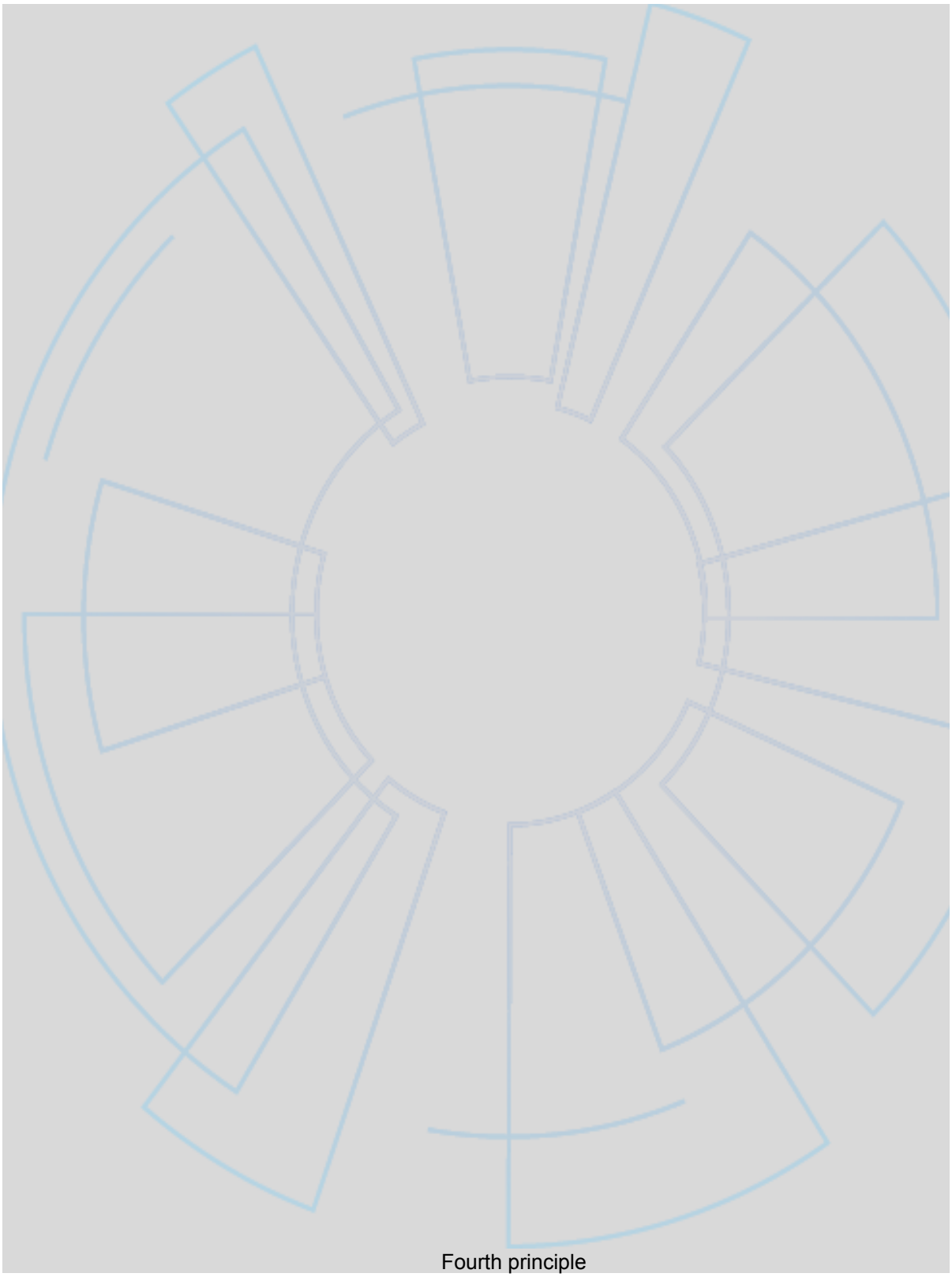
7.11 The third data privacy principle requires that personal data must be adequate, relevant and not excessive. You must, therefore, ensure:

7.11.1 you identify the personal data needed for a particular purpose and you collect the minimum amount required to properly fulfil that purpose. Care must be taken to avoid collecting excessive or irrelevant elements of personal data;

7.11.2 you do not hold personal data on a 'just-in-case' basis because you think it might be useful in the future but without having any clear idea of what that future purpose might be;

7.11.3 you keep personal data up to date (otherwise personal data which were originally adequate may cease to be so); and

7.11.4 you do not keep personal data for longer than the purposes for which it was originally collected unless there is a clear overriding business need or legal/regulatory requirement (otherwise that data may cease to be relevant and become excessive).



Fourth principle

Personal data must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that are inaccurate (having regard to the purpose(s) for which they are processed) are immediately deleted or rectified.

7.12 Personal data will be inaccurate if it is incorrect or misleading as to any matter of fact (e.g. an incorrect name or address). If you are inputting data onto our system and are unsure as to the accuracy of certain information (e.g. because you cannot read the handwriting or because it looks like an obvious mistake or omission), in the first instance speak to your line manager for guidance about how you can verify the accuracy of the information.

7.13 We will not be in breach of this principle, even if we are holding inaccurate personal data, if:

7.13.1 we accurately recorded those data when we received them from the Living Person or a third party, and

7.13.2 we took reasonable steps to ensure the accuracy of those personal data, and

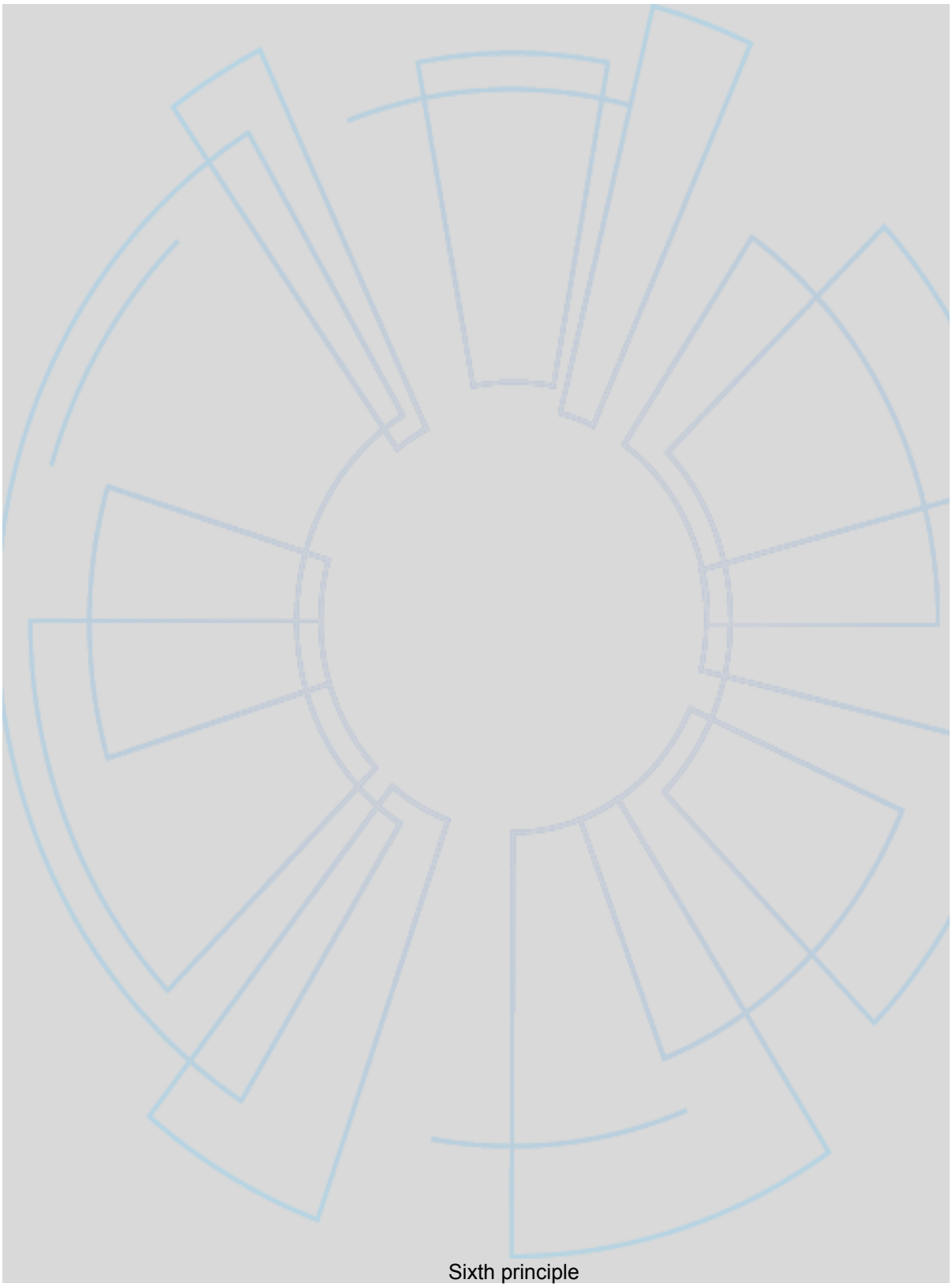
7.13.3 if the Living Person has notified us that the personal data are inaccurate, we have taken steps to indicate this fact (e.g. by making a note that we have received an objection).

7.14 You must take reasonable steps to keep personal data up to date to the extent necessary. The purpose for which personal data is held will determine whether it needs to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated.

Fifth principle

Personal data processed for any purpose(s) must not be kept for longer than is necessary for that/those purpose(s).

7.15 Personal data must not be retained for longer than the purpose(s) for which it was originally collected unless there is a clear overriding business need or legal/regulatory requirement to retain the personal data. You should review the personal data which you hold on a regular basis and delete any data which is no longer required in connection with the purpose for which it were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data. The <Company>'s Data Retention Policy **sets out the procedures for ensuring that documents/records are updated, archived and deleted appropriately as well as suggested timeframes for the retention of key categories of documents/records.**



Sixth principle

Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7.16 All Employees have a responsibility to help keep personal data secure. As set out in section 7.17.1 below, Employees should, in particular, be aware of the obligations and follow the recommendations in the Information Assets Security Policy **and the** Information Assets Acceptable Use Policy **Further, all Employees who have access to personal data must follow the** Employee Regulations Manual **and are under a legal responsibility to keep information confidential.**

7.17 This sixth data privacy principle requires the <Company> to take appropriate technical and organisational measures to protect the personal data which we process:

7.17.1 technical measures include: software controls to restrict user access; up-to-date virus checking software; audit trail software; encryption, all of which we manage through IT Security. In this regard please consult the Guideline on Technical and Organisational Measures **and read and comply with our** Information Assets Security Policy **and** Information Assets Acceptable Use Policy**; and**

7.17.2 organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; training Employees on the care and handling of personal data; all of which you are responsible for complying with and applying to your daily routine.

7.18 Where personal data is transmitted outside of the <Company>, for example to a third party service provider who may need to process personal data on our behalf, a secure medium must be used to transmit such data and a written agreement (containing the required level of security standards and data protection obligations) should be in place with each such third party prior to any disclosure of personal data to that third party. In all such instances, please ensure that you comply with our Third Party Data Sharing Process**. In addition, consideration should also be given as to whether a data privacy impact assessment should be carried out. Please refer to sections 8.7 to 8.10 of this Policy for further details about what a** Data Privacy Impact Assessment **is and when one should be carried out.**

Seventh principle

Personal data will at all times be processed in a manner that can demonstrate compliance with the above-mentioned data privacy principles.

7.19 This seventh data privacy principle requires us to demonstrate that we comply with all the above- mentioned data privacy principles and requirements and it is our responsibility to do so. We achieve this by various different methods, including:

7.19.1 implementing appropriate technical and organisational measures, such internal and external facing policies, procedures, processes, records and notices, that meet data privacy principles/requirements and comply with all applicable data privacy laws;

7.19.2 using data privacy impact assessments, where appropriate; and

7.19.3 accurately documenting our processing activities.

8. DATA PRIVACY REQUIREMENTS EXPLAINED

Rights of Living Persons

8.1 Living Persons generally have the ability to have access to their personal data on request and may also be entitled to a number of other rights as set out earlier in clause 6.2.1 including preventing the processing of their personal data or having it erased. Requests from Living Persons should be handled in accordance with the <Company> Data Subject Access Request Process**.**

8.2 If you receive a request in writing from a Living Person mentioning any of the rights set out in clause 6.2.1, you must notify the Data Privacy Office of such request immediately and, at the Data Privacy Office's direction, ensure you prepare your response to the request promptly and completely as there are strict timescales within which we must respond.

Transferring Personal Data Overseas

8.3 Particular care must be taken when Personal Data is transferred to a country or territory other than the country where either:

8.3.1 the Living Person from which it was originally collected is resident; or

8.3.2 the <Company> entity that collected it is established.

8.4 Generally, personal data originating in the European Economic Area ("EEA**") must not be transferred outside of the EEA, unless there is a mechanism for ensuring adequate level of protection for the rights and freedoms of Living Persons in relation to the processing of personal data or the transfer is necessary for the performance of a contract (concluded for the benefit of the Living Person).**

8.5 Please be aware that transfers may take place that are not obvious. For example, if an approved service provider of the <Company>, who processing personal data on our behalf, sub-contracts some of its processing obligations to a third party outsource provider in India, there will be a transfer

of personal data out of the EEA (i.e. from the approved service provider of the <Company> (who is our data processor) to the third party outsource provider

(who is a sub-processor) which will be prohibited unless certain conditions are met).

8.6 Managing overseas data transfers in accordance with these principles requires particular care. Where any personal data is proposed to be transferred to another country or outside of the EEA, please consult with the Data Privacy Office who will advise on how to comply applicable data transfer restrictions.

Data Privacy Impact Assessments

8.7 Where a new project or way of working, or proposed changes to an existing project or way of working, involve intensive or higher risk processing of personal data or sensitive personal data, a data privacy impact assessment should be carried out

8.8 It is the <Company> policy to carry out data privacy impact assessments before launching any new project or way of working (or making changes to an existing project or way of working) which uses significant quantities of personal data, processes sensitive personal data, or processes personal data in novel or high risk ways.

8.9 A data privacy impact assessment is important for us to identify and mitigate privacy risks before a project launches, and to apply the principles of "privacy by design" and "privacy by default", whereby projects are built with privacy compliance in mind. This can save time and resource by preventing intervention at a later date. Please refer to our Privacy by Design and Privacy by Default Guideline **to understand how to apply these principles.**

8.10 The Data Privacy Office is responsible for determining when a data privacy impact assessment is required, for completing certain parts of the assessment and for signing-off on its findings. However, the responsibility for identifying a project which may be in scope for an assessment rests with the business, and with the owner of that project. Please refer to our Data Privacy Impact Assessment **for a data privacy impact assessment template and guidance in preparing an assessment.**

Data Breaches

8.11 All losses of personal data should be contained and remedied as soon as possible and where necessary all appropriate stakeholders informed of the data breach.

8.12 A data breach is an incident which involves an unauthorised or inappropriate disclosure of, or access to, personal data. Examples of data breaches include: third party attacks on IT infrastructure designed to harvest personal data for criminal purposes; accidental loss or theft of <Company> devices (e.g. mobile phones, laptops, USB devices); the passing to third parties or disposal of personal information without appropriate security measures being in place.

8.13 All Employees have an obligation to report data breaches (or suspected data breaches) to the Data Privacy Office. Please refer to our Data Security Incident Response Plan **which provides further details on how data breaches should be managed and resolved.**

9. CONSEQUENCES OF NON-COMPLIANCE AND ACCOUNTABILITY

9.1 If we are found to be in breach of applicable data privacy laws and regulations, data privacy supervisory authorities may impose monetary penalties, or issue

other enforcement proceedings against us which could result in our being prevented from further use of the affected personal data, or being required to change our processing procedures, or having other conditions imposed upon us in respect of the processing of personal data. Enforcement action will usually have a cost and time implication for the business. However, more damaging might be any restrictions imposed upon us which prevent us from exploiting our databases commercially.

9.2 Additionally, the associated publicity could make us appear as an organisation that does not respect the privacy rights of individuals and cause us reputational damage.

9.3 Affected Living Persons may also take legal action against us and claim compensation for any breaches of applicable data privacy laws and regulations on our part that have resulted in damage (or damage and distress) to the Living Person.

9.4 Periodic monitoring of adherence to this Policy takes place to help ensure compliance with this Policy, applicable data protection laws and/or contractual agreements in connection with the handling of personal data. As set out earlier in this Policy, it is the responsibility of all Employees to assist the <Company> to comply with this Policy. It is therefore key that all Employees familiarise themselves with both this Policy and apply their provisions in relation to all processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal.

10. POLICY OWNERSHIP AND RESPONSIBILITY

10.1 The owner of this Policy is the Data Privacy Office., The Data Privacy Office shall ensure that this Policy is properly applied across the <Company> and is responsible for the oversight and implementation of this Policy.

10.2 The Data Privacy Office is responsible for communicating Policy requirements and any revisions made to this Policy.

11. MONITORING AND COMPLIANCE HANDLING

11.1 This Policy shall be monitored to ensure its effectiveness.

11.2 The Policy owner will report to the Presidents relevant breaches of and exceptions to this Policy as soon as possible. Internal Audit shall also review compliance with this Policy as part of its audit reviews and report exceptions to this Policy to the Presidents and the Policy owner.

11.3 An annual report on compliance with this Policy and on the effectiveness of the systems in place to manage the non-compliance risk, together with a list of breaches, will be presented to our Presidents by the Data Privacy Office.

11.4 Failure to comply with the minimum standards may be reported to the Presidents and treated as a disciplinary matter under our disciplinary procedures and could potentially lead to dismissal.

12. POLICY REVIEW CYCLE

12.1 This Policy shall be reviewed periodically to ensure that the Policy is meeting all of its objectives.

12.2 Changes to applicable data protection laws, regulation or regulatory regimes, together with the <Company> risk profile in the global operating environment, may form triggers for revisions or updates to this Policy.

12.3 It is the responsibility of all Employees to assist the <Company> to comply with this Policy.

13. QUERIES AND WAIVER

13.1 For core businesses (<Company>, <Company> and <Company> World), the Data Privacy Office is available to help give constructive advice on this Policy in consultation with <Company> Legal who will advise on legal issues.

13.2 Any instances where a waiver of this Policy is sought must first be reported to the Data Privacy Office.