ZEDRA

PRIVACY AND DATA PROTECTION POLICY
ZEDRA GLOBAL SERVICES (UK) LIMITED AND AFFILIATES

1. Policy Summary

1.1. We are committed to complying with all relevant UK and EU laws in respect to data privacy and how we collect and process personal data. To that end, the Senior Management have developed and implemented and will maintain and continuously improve a documented Information Security Management System (**ISMS**).

1.2. In this document, references to **us**, **we**, **our** means ZEDRA Global Services (UK) Limited, ZEDRA Client Accounts (UK) Limited, ZEDRA Corporate Reporting Services (UK) Limited and any other subsidiary within this group of companies.

1.3. This policy sets out the basis upon which we process personal data and the obligations on Workers in assisting us to comply with our corporate and legal obligations. Any questions about this policy should be sent to the Data Protection Officer.

1.4. This policy should be read in conjunction with our Data Security Policy.

2. Scope

2.1. The Data Protection Legislation (as defined below) is designed to protect the "rights and freedoms" of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

2.2. Our Information Security Team is responsible for the ongoing maintenance, effectiveness and ultimate alignment of this policy with our legal/regulatory requirements.

3. Definitions

3.1 **Data controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK, European Union (**EU**) or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

3.2 **Data Protection Legislation** - applicable privacy and data protection laws including EU GDPR, UK GDPR, Data Protection Act 2018 and any applicable implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

3.3 **Data Protection Officer** - means Alexandra Womphrey (or such other person as we may update on this site from time to time)and can be contacted in writing at ZEDRA Global Services (UK) Limited, New Penderel House 4th Floor, 283-288 High Holborn, London WC1V 7HP.

3.4 **Data subject** – any living individual who is the subject of personal data held by us.

3.5 **Data subject consent** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

3.6 **Establishment** – the main establishment of the controller in the UK and/or EU (as applicable) will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the UK and/or EU (as applicable) will be its administrative centre. If a controller is based outside the UK and/or EU (as applicable), it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

3.7 **EU GDPR** - the General Data Protection Regulation (*(EU) 2016/679).*

3.8 GDPR – the EU GDPR and/or the UK GDPR (as applicable).

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

3.10 **Profiling** – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

3.11 **Personal data breach** – a breach of security leading to the accidental or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

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

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

3.14 **Territorial scope** – the GDPR will apply to all controllers that are established in the UK and/or EU (as applicable) who process the personal data of data subjects. It will also apply to controllers outside of the UK and/or EU (as applicable) that process personal data to offer goods and services or monitor the behaviour of data subjects who are resident in the UK and/or EU (as applicable).

3.15 **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3.16 **UK GDPR** - Regulation (EU) 2016/679 General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019;

3.17 **Worker** – any staff, employee, director, worker, contractor or other third party appointed by us.

4 Objectives of the ISMS

4.1 ISMS will ensure that we:

4.1.1 meet our own privacy requirements as a data controller;

4.1.2 meet all necessary compliance obligations as per the Data Protection Legislation;

4.1.3 impose controls in line with our risk management strategy;

4.1.4 meet all applicable statutory, regulatory, contractual and professional duties; and

4.1.5 protect the interests of data subjects, third parties, affiliated data processors and other interested parties.

4.2 We are committed to ensuring our compliance to Data Protection Legislation. In particular we will ensure that we are:

4.2.1 processing personal data only where this is strictly necessary for legitimate business purposes;

4.2.2 collecting only minimum personal data required for these purposes and not processing excessive personal information;

4.2.3 providing clear information to individuals about how their personal data will be used and by whom;

4.2.4 only processing relevant and adequate personal data;

4.2.5 processing personal data fairly and lawfully;

4.2.6 maintaining an inventory of the categories of personal data processed by us, as both data controller and processor;

4.2.7 maintaining its accuracy and, where necessary, kept up to date;

4.2.8 retaining personal data only for as long as is necessary for both legal and/or regulatory reasons or, for other legitimate purposes – expressly agreed;

4.2.9 respecting an individuals' rights in relation to their personal information, including their right to access;

4.2.10 maintaining its security and accessibility;

4.2.11 only transferring personal data outside the UK, EU and/or other countries deemed adequate by the UK/EU (as applicable) in circumstances where it can be adequately protected and is necessary;

4.2.12 appropriately apply the various exemptions allowable by Data Protection Legislation;

4.2.13 developing and implementing an ISMS to enable the policy to be implemented effectively;

4.2.14 where appropriate, identifying both internal and external stakeholders and the degree to which these stakeholders are involved in the governance of our ISMS;

4.2.15 the identification of stakeholders with specific responsibility and accountability for the ISMS.

5 Notification

5.1 All of the companies in our group are (where applicable) registered with the Information Commissioner as a data controller.

5.2 A copy of the ICO notification details are retained by the Data Protection Officer.

5.3 This policy applies to all Workers. Any breach of the Data Protection Legislation or the ISMS will be dealt with under our disciplinary policy and/or any appropriate contract and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

5.4 Partners and any third parties working with or for us who have or may have access to personal data will be expected to have read, understood and comply with this policy. No third party may access personal data held by us without having first entered into a relevant data protection and confidentiality agreement with us.

6 Responsibilities

6.1 We act as both a data controller and data processor under the Data Protection Legislation.

6.2 Senior Management and all those in managerial or supervisory roles with us are responsible for developing and encouraging correct information handling practices, responsibilities of which are set out within staff handbooks.

6.3 The Information Security Team is accountable to Senior Management directly for the management of personal data use and for ensuring overall compliance with Data Protection Legislation and best practice can be demonstrated. These accountabilities include the:

6.3.1 development and implementation of the ISMS as required by this policy; and

6.3.2 security and risk management in relation to compliance with the policy.

6.4 The Information Security Team, have been appointed to take overall responsibility for our compliance with this policy and the day to day management and, in particular, have direct responsibility for ensuring that we comply with Data Protection Legislation.

6.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request procedure and is the first point of call for Workers seeking clarification on any aspect of data protection compliance.

6.6 Compliance with data privacy legislation is the responsibility of all our Workers who process personal data.

6.7 Workers are responsible for ensuring that any personal data supplied by them and that is about them, is accurate and up to date.

7 Risk Assessment

7.1 To ensure that we are aware of any risks associated with the processing of the variable types of personal data we hold and process, we have put in place certain procedures as set out below.

7.2 We have a process for assessing the level of risk to individuals associated with the processing of their personal data. Assessments will also be carried out in relation to processing tasks undertaken by other organisations on our behalf. We shall manage any risks which are identified by the risk assessment to reduce the likelihood of a non-conformance with this policy.

7.3 Where a type of processing, uses new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the “rights and freedoms” of natural persons, we shall consider the affect of the envisaged processing operations on the protection of personal data.

7.4 A single assessment may address a set of similar processing operations that present similar high risks.

7.5 Where, as a result of any impact assessment, it is clear that we are about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not we proceed will be escalated for review to the appointed Data Protection Officer who shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioners Office.

7.6 Appropriate controls will be selected, and applied to reduce the level of risk associated with processing personal data to an acceptable level, by reference to our documented risk acceptance criteria and the requirements of the Data Protection Legislation.

8 Data protection principles

8.1 All processing of personal data must be done in accordance with the following data protection principles:

8.1.1 Personal data must be processed lawfully, fairly and transparently.

8.1.2 Demonstrate transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals’ “rights and freedoms”. Information must be communicated to the data subject in an intelligible form using clear and plain language.

8.1.3 The specific information that must be provided to the data subject must as a minimum include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

8.1.4 Personal data can only be collected for specified, explicit and legitimate purposes;

8.1.5 Personal data must be adequate, relevant and limited to what is necessary for processing;

8.1.6 The Data Protection Officer is ultimately responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected;

8.1.7 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the appointed Data Protection Officer;

8.1.8 The Information Security Team will ensure that, on an annual basis all data collection methods are reviewed by internal auditors to ensure that collected data continues to be adequate, relevant and not excessive;

8.1.9 If data is given or obtained that is excessive or not specifically required by us – as per the documented procedures, the appointed Data Protection Officer is ultimately responsible for ensuring that it is securely deleted or destroyed in line with internal policies;

8.1.10 Personal data must be accurate and kept up to date;

8.1.11 Data that is kept for a prolonged period of time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate;

8.1.12 The Practice Manager is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it;

8.1.13 It is also the responsibility of individuals to ensure that data held by us is accurate and up to date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.

8.2 Clients should notify us of any changes in circumstance to enable personal records to be updated accordingly. It is our responsibility to ensure that any notification regarding change of circumstances is noted and acted upon.

8.3 The Information Security Team is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

9 Personal Data Format

9.1 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

9.2 Where personal data is retained beyond the processing date, it will be encrypted or anonymised in order to protect the identity of the data subject in the event of a data breach.

9.3 Personal data will be retained in line with the retention of records policies and, once its retention date is passed, it must be securely destroyed.

9.4 The Information Security Team must specifically approve any data retention that exceeds the retention periods defined and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

10 Data Processing

10.1 Personal data must be processed in a manner that ensures its security.

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

10.3 These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

10.4 Our compliance with this principle is contained in our Information Security Management System (ISMS).

10.5 Security controls will be subject to audit and review.

10.6 Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

10.7 The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

11 Safeguards

11.1 An assessment of the adequacy by the data controller of its safeguards are carried out, addressing the following factors:

11.1.1 the nature of the information being transferred;

11.1.2 the country or territory of the origin, and ultimate destination, of the information;

11.1.3 how the information will be used and for how long.

12 Accountability

12.1 The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

12.2 Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform (where relevant) impact assessments, comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

13 Data subjects' rights

13.1 Data subjects have the following rights regarding data processing and the data that is recorded about them:

13.1.1 to make subject access requests regarding the nature of information held and to whom it has been disclosed;

13.1.2 to prevent processing likely to cause damage or distress;

13.1.3 to prevent processing for purposes of direct marketing;

13.1.4 to be informed about the mechanics of automated decision taking process that will significantly affect them;

13.1.5 not to have significant decisions that will affect them taken solely by automated process;

13.1.6 to sue for compensation if they suffer damage by any contravention of the GDPR;

13.1.7 to take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data;

13.1.8 to request the ICO to assess whether any provision of the GDPR has been contravened;

13.1.9 the right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;

13.1.10 the right to object to any automated profiling without consent.

13.2 Data subjects may make data access requests.

14 Complaints

14.1 Data Subjects who wish to complain to us about how their personal data has been processed may lodge their complaint directly with the Data Protection Officer. All complaints should be done in writing.

14.2 Data subjects may also complain directly to the Information Commissioners Office.

15 Consent

15.1 We understand 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

15.2 We understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

15.3 In most instances consent to process personal and sensitive data is obtained routinely by us using standard consent documents e.g. when a new member of staff signs a contract of employment.

16 Security of data

16.1 All Workers are responsible for ensuring that any personal data which we hold and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into a contracted agreement.

16.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with our access control policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

16.2.1 in a lockable room with controlled access; and/or

16.2.2 in a locked drawer or filing cabinet; and/or

16.2.3 if computerised, password protected in line with corporate requirements in the Access Control Policy.

16.3 Care must be taken to ensure that PC screens, tablets and terminals are not visible except to authorised Workers.

16.4 Any personal data that is removed from our offices should be kept secure and not left in any visible or insecure place. In no circumstances should any personal data be left unattended in cars or vehicles.

16.5 Manual records may not be left where they can be accessed by unauthorised personnel. As soon as manual records are no longer required for day-to-day client work they must be securely disposed.

16.6 Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

16.7 All Workers MUST report any breach of this policy as soon as they become aware of it to the Data Protection Officer.

17 Rights of access to data

17.1 Data subjects have the right to access any personal data (i.e. data about them) which is held by us in electronic format and manual records which form part of a relevant filing system.

17.2 Subject Access Requests are dealt with by the Data Protection Officer and anyone nominated to act on their behalf.

18 Disclosure of data

18.1 We take all appropriate steps to ensure that personal data is not disclosed to unauthorised third parties. All Workers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of our business.

18.2 The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

18.2.1 to safeguard national security;

18.2.2 prevention or detection of crime including the apprehension or prosecution of offenders;

18.2.3 assessment or collection of tax duty;

18.2.4 discharge of regulatory functions (includes health, safety and welfare of persons at work);

18.2.5 to prevent serious harm to a third party;

18.2.6 to protect the vital interests of the individual, this refers to life and death situations

18.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

19 Disposal of records

19.1 Personal data must be disposed of in a way that protects the “rights and freedoms” of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.