Global Privacy Policy

Introduction

ICAS World and its subsidiary companies and branches (referred to as "ICAS" in this policy) supports organisations through the promotion of the health and wellbeing of their employees, while at the same time improving productivity and reducing absence. We have been an Employee Assistance Programme (EAP) provider since 1987 and today, we are one of the major global players in the sector. We are committed to ensuring your privacy and personal information is protected.

What is Data Protection Law?

Data protection law gives individuals certain rights about the way in which their personal data is processed. If organisations do not comply with data protection law, they may be subject to sanctions and penalties imposed by the national data protection authorities and the courts. When ICAS processes personal data, this activity and the personal data in question are covered and regulated by data protection law. The General Data Protection Regulation ("GDPR") (EU) 2016/679 ("GDPR") is a regulation in European Union law on data protection and privacy for all individuals within the European Union, and the UK has retained a version of it. The Protection of Personal Information Act 2013 ("POPIA") is a South Africa law on data protection and privacy for all individuals within South Africa. Both laws address the transfer of personal data outside their borders.

Data Privacy Policy

This ICAS Data Privacy Policy (Global) ("Policy") establishes ICAS's approach to compliance with GDPR and POPIA. Where local laws and regulations mandate additional restrictions on the collection, use and disclosure of personal data that exceed those contained in this Policy, the local laws and regulations will prevail.
This Policy describes how personal data must be processed to meet ICAS's data protection standards and to comply with privacy laws and regulations. Additional instructions and / or guidelines regarding personal data processing activities at ICAS are provided to ICAS employees in internal policies.

What does this mean for ICAS?

ICAS must take proper steps to ensure that it processes personal data on an international basis in a safe and lawful manner. ICAS has therefore developed policies and procedures to ensure appropriate governance and compliance with such data privacy laws, including GDPR and POPIA. Such framework shall apply to all personal data processing activities conducted by ICAS globally.

Data Protection Principles

Below is the summary of basic data protection principles that ICAS must observe when it processes personal data.

Principle 1 – lawfulness of processing, fairness and transparency

- ICAS will ensure that all processing is carried out in accordance with applicable laws.
- ICAS will inform and explain to individuals, at the time when their personal data is collected, how their personal data will be processed.

Principle 2 – purpose limitation

- ICAS will only obtain and process personal data for those purposes which are known to the individual or which are within their expectations and are relevant to ICAS.
- ICAS will only process personal data for specified, explicit and legitimate purposes and not further process that information in a manner that is incompatible with those purposes unless such further processing is consistent with the applicable law of the country in which the personal data was collected.

How do we collect your personal information?	We collect personal information directly from you: • using our EAP services generally and which may be telephonically, via e-mail through the web, mobile or web applications, any other internet based application or in person; • when you contract with ICAS to provide services on our behalf or where we agree to provide services on your behalf. • via cookies. You can find out more about this in our Cookie Policy; • through feedback forms; • via our telephone calls with you, which may be recorded; • when you provide your details to us either online or offline; • when you respond to any job advertisement or are employed by ICAS We also collect your personal information from many different sources including third parties such as: • your employer • medical professionals

Principle 3 – data minimisation

- ICAS will ensure that data collected and processed is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

What personal information do we collect?	As the data controller / responsible party, joint data controller and/or data processor / operator, ICAS may collect and process the following information about you:
	• **Personal information**
	  ○ contact, gender details such as name, email address, postal address and telephone number
	  ○ factors specific to physical, physiological, economic, cultural or social identity
	  ○ call recordings
	  ○ information obtained through our use of cookies. You can find out more about this in our Cookie Policy.
	
	• **Sensitive personal information**
	  ○ details of your current or former physical or mental health
	  ○ details regarding criminal offences, including alleged offences, criminal proceedings, court judgments, outcomes and sentences
	  ○ details concerning sexual life or sexual orientation, for example marital status

Principle 4 –accuracy

- ICAS International will keep personal data accurate and up to date.

Principle 5 – limited retention of personal data

- ICAS will only keep personal data for as long as is necessary for the purposes for which it is collected and further processed and to comply with our legal and regulatory obligations. The time we retain your personal information for, will differ depending on the nature of the personal information and what we do with it. In some cases, such as if there is a dispute or a legal action we may be required to keep personal information for longer.

- Call recordings are kept securely and confidentially deleted within 6 months of collection.

- Your personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by data protection law in order to safeguard the rights and freedoms of individuals.

Principle 6 – integrity and confidentiality (security)

- ICAS will implement appropriate technical and organisational measures to ensure a level of security of personal data that is appropriate to the risk for the rights and freedoms of the individuals.

- ICAS will ensure that providers of services to ICAS also adopt appropriate and equivalent security measures.

- ICAS will comply with data security breach notification requirements as required under applicable law.

- ICAS will ensure that information is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

How do we use your personal information?	We use your personal information to provide you with the services you require based on your situation. So, if you have a problem, we make sure the right network of providers and specialists are in place. However, there are many other reasons why we use your personal information. Under data protection laws we need a reason to use and process your personal information and this is called a legal basis. We have set out below the main reasons why we process your personal information and the applicable circumstances when we will do so. When the personal information we process about you is classed as sensitive personal information (such as details about your health, sexual orientation or criminal offences) we must have an additional legal ground for such processing. Legal grounds are as follows. • Processing is necessary for us to provide you with the services you require, such as assessing your need and setting you up as a user of the services and communicating with you. • We have a legal or regulatory obligation to use such personal information, for example, when the relevant data protection regulator requires us to maintain certain records of any dealings with you. • We need to use your personal information to establish, exercise or defend our legal rights, for example when we are faced with any legal claims or where we want to pursue any legal claims ourselves. • We need to use your personal information for reasons of substantial public interest, such as investigating fraudulent or criminal activities. • In certain instances, you may elect to use our EAP services anonymously. However, where necessary we will ask for your consent in relation to processing your sensitive personal information (such as health data) such as where you are in a safety-critical role. This will be made clear when you provide your personal information. We will ask for your consent and explain why it is necessary. Without your consent in these

	circumstances, we may not be able to provide you with some of our services. Where you provide sensitive personal information about a third party we will ask you to confirm that the third party has provided his or her consent. • We have appropriate legitimate business need to use your personal information (such as call recordings) to maintain our business records, developing and improving our products and services to train our staff and complaints handling all while ensuring that such business need does not interfere with your rights and freedoms and does not cause you any harm. • We need to use your sensitive personal information such as health data because it is necessary for your vital interests, this being a life or death matter.

Principle 7 – rights of individuals

- ICAS will adhere to the data subject rights procedure and will respond to any requests from individuals to access their personal data in accordance with applicable law.

- ICAS will also deal with requests to rectify or erase inaccurate or incomplete personal data, or to cease processing personal data in accordance with the data subject rights procedure.

The right to access your personal information	You are entitled to a copy of the personal information we hold about you and certain details of how we use it. In Europe, there will not usually be a charge for dealing with these requests**.** Your personal information will usually be provided to you in writing, unless otherwise requested, or where you have made the request by electronic means, in which case the information will be provided to you by electronic means where possible. For requests for access to medical records, we will provide a summary of clinical interactions.
The right to rectification	We take reasonable steps to ensure that the personal information we hold about you is accurate and complete. However, if you do not believe this is the case, please contact us and you can ask us to update or amend it.
The right to erasure	In certain circumstances, you have the right to ask us to erase your personal information, for example where the personal information we collected is no longer necessary for the original purpose or where you withdraw your consent. However, this will need to be balanced against other factors, for example according to the type of personal information we hold about you and why we have collected it, there may be some legal and regulatory obligations which mean we cannot comply with your request. Please note that if you withdraw your consent we may not be able to provide you with the services you have requested.
Right to restriction of processing	In certain circumstances, you are entitled to ask us to stop using your personal information, for example where you think that the personal information we hold about you may be inaccurate or where you think that we no longer need to process your personal information.
Right to data portability	In certain circumstances, you have the right to ask that we transfer any personal information that you have provided to us to another third party of your choice. Once transferred, the other party will be responsible for looking after your personal information.

Right to object to direct marketing	You can ask us to stop sending you marketing messages at any time.
Right not to be subject to automated-decision making	Some of our decisions are made automatically by inputting your personal information into a system or computer and the decision is calculated using certain automatic processes rather than our employees making those decisions.
The right to withdraw consent	For certain uses of your personal information, we will ask for your consent. Where we do this, you have the right to withdraw your consent to further use of your personal information. Please note in some cases we may not be able to deliver the services you require if you withdraw your consent.
The right to make a complaint	You have a right to complain to the relevant regulator at any time if you object to the way in which we use your personal information. More information can be found on regulators' websites — the Information Commissioner's Office website https://ico.org.uk/ for the UK, the Information Regulator's website for South Africa https://www.justice.gov.za/inforeg/

Principle 8 – ensuring adequate protection for trans-border transfers

- ICAS is a global business. To offer our services, we may need to transfer your personal data to companies within the ICAS Group of companies and with third parties in other countries.

- ICAS will not transfer personal data that is subject to GDPR to third parties outside European Economic Area ("EEA") or Switzerland without ensuring adequate protection.

- ICAS will not transfer personal data that is subject to POPIA to third parties outside South Africa without ensuring adequate protection.

Who do we share your personal information with?	We might share your personal information with two types of organisations – companies within the ICAS group of companies, i.e. parent companies, subsidiary and affiliated (sister companies) ("Group"), and other third parties outside the Group. We won't share any of your personal information other than for the purposes described in this Privacy Policy and if we share anything outside the Group, it will be kept strictly confidential and will only be used for reasons that we have agreed in advance.

Principle 9 – safeguarding the use of sensitive personal data

- ICAS will only process sensitive personal data where an individual elects to disclose same, alternatively where ICAS has a legitimate basis for doing so, consistent with the applicable law of the country in which the personal data was collected.

- Additional security measures and safeguards will be implemented to ensure that this sensitive personal data remains confidential and that it is deleted as soon as is reasonably possible.

Principle 10 – accountability

- ICAS takes responsibility for compliance with the other data protection principles.

- ICAS implements appropriate technical and organisational measures, including record keeping, in order to be able to demonstrate compliance.

Legally Binding Effect of This Policy

ICAS and its employees (including new hires, individual contractors and temporary staff) that process personal data worldwide must comply with, and respect, this Policy when processing personal data as a controller and / or processor, irrespective of the country in which they are located.

ICAS reserves the right to change, modify or update this Policy at any time. Please review it frequently for any updates.

Contact Details

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues, you can contact the ICAS Data Privacy Office at the address below who will either deal with the matter or forward it to the appropriate person or department within ICAS.

Please note that in some cases we may not be able to comply with a request relating to your rights under this policy for reasons such as our own obligations to comply with other legal or regulatory requirements. However, we will always respond to any request you make within one month and if we can't comply with your request, we will tell you why. In some circumstances exercising some of these rights (including the right to erasure, the right to restriction of processing and the right to withdraw consent) will mean we are unable to continue providing you the services you have selected and may therefore result in the cancellation thereof.

Attention: Lindsay West – Data Privacy Officer
Email: dpo@icasworld.com
Address: ICAS International Holdings Ltd, 85 Gresham Street, London, EC2V 7NQ
To log a Data Subject Access Request, e-mail datasubjectrequest@icasworld.com (Europe) or paia@icas.co.za (South Africa). Note that we will require proof of identification (passport or driver's license) and a utility bill to confirm that you are the Data Subject.

1. "**ICAS**" includes ICAS International Holdings including ICAS Gulf (branch), ICAS Spain (affiliated subsidiary), ICAS Southern Africa (subsidiary) and designated third parties ("Group Members").
2. "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
3. "**Personal data**" / "**Personal information**"means 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.
4. "**Sensitive personal data**" means "special categories of personal data" as set out in GDPR and POPIA, which must be treated with extra security. These categories include health information and also genetic data and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
5. For the purpose of this Policy, reference to Europe means the EEA and Switzerland.
6. This policy is drafted in the English language only.