HUMAN RIGHTS AT SEA
DATA PROTECTION POLICY

ISSUED: 03/12/2018

Prepared for HRAS by Mishcon de Reya

PURPOSE

This policy sets out how Human Rights at Sea (HRAS) expects personal data to be used within the business. Personal data is a valuable commodity and we all need to take all the steps we can to make sure we use all personal data properly and lawfully (whether the data relates to colleagues, clients or suppliers).

This Data Protection Policy applies to all Personal Data we *process* regardless of the media on which, or the format in which, that data is stored. For the purposes of this policy, processing means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties such as service providers.

If you have any questions about the policy, please contact David Hammond, who is the current Data Owner for HRAS.

POLICY DEFINITIONS

Company Personnel	The set of individuals comprising HRAS permanent employers, contractors, suppliers, partners, HRAS Holdings Limited group members, contractors, and non-executive directors with access to HRAS Systems and/or data for the purposes of providing or supporting the firm's day to day business and any other associated activities.
Data Owner	The HRAS data owner is the individual holding organisation responsibility for data across the organisation, as well as having overall responsibility for data protection compliance within HRAS.
Data Controller	HRAS is the Data Controller of all Personal Data relating to our Company Personnel, as well as all Personal Data used in the business for our own commercial purposes.
Data Subject	A living, identified or identifiable individual about whom we hold Personal Data.
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (*(EU) 2016/679*).

Personal Data	Personal data as referred to in this standard should be considered to be defined as in the General Data Protection Regulation 2016/679 (GDPR). The standard defines personal data as follows: *'personal data' 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.*
Personal Data Breach	Any act or omission that compromises the security or availability of Personal Data or the safeguards that we or our third-party service providers put in place to protect it. The loss of, or unauthorised access to, Personal Data may amount to a Personal Data Breach.
Personnel	All employees, workers contractors, agency workers, consultants, directors, members and other people engaged to provide personal services on the Company's behalf.
Privacy Notices	Separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.
Pseudonymisation	Replacing information that identifies an individual with one or more artificial identifiers or pseudonyms so that the individual cannot be identified without the use of additional information which is meant to be kept separately and secure.
Sensitive Personal Data	Sensitive personal data within HRAS is data which falls into one of two categories: Firstly, data which falls under the description of sensitive personal data within the GDPR, including information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. Secondly, any personal data relating to real or potential HRAS investigations relating missing persons, violations of human rights, or any other sensitive matters which require anonymity or high levels of confidentiality.

SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The Data Owner is responsible for overseeing this Data Protection Policy. Please contact the Data Owner with any questions about this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being complied with.

PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the data protection principles set out in the GDPR which require Personal Data to be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected only for specified, explicit and legitimate purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) accurate and where necessary kept up to date;

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed;

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;

(g) not transferred to another country without appropriate safeguards being in place; and

(h) made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

LAWFULNESS, FAIRNESS, TRANSPARENCY

1.2 **Lawfulness and fairness**

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her consent;

(b) the processing is necessary for the performance of a contract with the Data Subject (such as the performance of the employment contract);

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests.

1.3 **Consent**

A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis for processing, explicit consent is usually required for processing Sensitive Personal Data, for automated decision-making and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of Sensitive Data. Where explicit consent is required the consent must be a very clear and specific statement and should be accompanied by a notice explaining the reasons for the processing and how the Sensitive Data will be processed; this is typically communicated via a Privacy Notice that can be given to the Data Subject.

You will need to evidence consent and keep records of all consents so that the Company can demonstrate compliance with consent requirements.

1.4 **Transparency**

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we will provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and Data Owner, how and why we will use, process, disclose, protect and retain that Personal Data through a Privacy Notice.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that Personal Data.

If you need further guidance please contact the Data Owner for further information.

PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. You cannot use Personal Data for new, different or incompatible purposes from that disclosed

when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process or collect Personal Data when your role requires it. You must not process or collect Personal Data for any reason unrelated to your role.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised. If you need further guidance please contact the Data Owner for guidance.

ACCURACY

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data, although you should contact the Data Owner if you are in any doubt about whether to destroy or amend such information.

STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

DATA SECURITY

1.5 Protecting personal data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. These controls are specified in the HRAS Data Handling Standard.

Our data controls have been assembled to protect the sensitive data that we retain, and must be used appropriately. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data.

You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

(b) integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with, and not attempt to circumvent, the safeguards we implement and maintain to protect Personal Data.

1.6 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Owner or any team or individual designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach. Failure to notify a suspected Personal Data breach may be a disciplinary offence that could lead to a range of sanctions, up to and including summary termination of your employment on grounds of gross misconduct.

TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

(c) the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject and, in some limited cases, for our legitimate interest.

In addition to the above, you must ensure that the Data Owner for the data in question is aware of and has approved this transfer prior to it taking place. If you need further guidance please contact the Data Owner for guidance.

DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have qualified rights when it comes to how we handle their Personal Data. These include rights to:

(e) withdraw consent to processing;

(f) receive certain information about the Data Controller's processing activities;

(g) request access to the Personal Data that we hold;

(h) prevent our use of their Personal Data for direct marketing purposes;

(i) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or to rectify inaccurate data;

(j) restrict or challenge processing in specific circumstances;

(k) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(l) object to decisions based solely on automated processing, including profiling (ADM);

(m) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

(n) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(o) make a complaint to the supervisory authority; and

(p) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your supervisor or the Data Owner.

ACCOUNTABILITY

1.7 Implementation

The Data Controller will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

The Company will ensure and document GDPR compliance by:

(a) appointing a suitably qualified Data Owner and an executive accountable for data privacy;

(b) implementing privacy by design when processing Personal Data and completing data protection impact assessments where processing presents a high risk to rights and freedoms of Data Subjects;

(c) training Personnel on the GDPR and data protection policies and maintaining records of such training; and

(d) testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

1.8 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

If applicable, you must keep and maintain accurate corporate records reflecting our processing including records of Data Subjects' consents and procedures for obtaining consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the Data Owner, clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

1.9 Training and audit

We are required to ensure all Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

1.10 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement appropriate technical and organisational measures in an effective manner to ensure compliance with data privacy principles (privacy by design).

You must assess what privacy by design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the cost of implementation;

(b) the nature, scope, context and purposes of processing; and

(c) the risks to rights and freedoms of Data Subjects posed by the processing.

Further to this, we must also conduct data protection impact assessments (DPIA) in respect to high risk processing.

You should conduct a DPIA (and discuss your findings with the Data Owner) when implementing major system or business change programs involving the processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) automated processing including profiling and automated decision making (ADM);

(c) large scale processing of Sensitive Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

1.11 Automated processing (including profiling) and automated decision-making

Automated Decision Making (ADM) takes place when a decision is made based solely on automatic processing (i.e. by the use of filtering software) which produces legal effects or significantly affects an individual.

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has explicitly consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being subject to automated processing, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on automated processing (including profiling), then Data Subjects must be informed, when you first communicate with them, of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken.

1.12 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

1.13 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company HRAS Global Holdings along with its subsidiary companies) if the recipient has a job-related need to know and the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.