H2O
Asset Management

H2O AM

Data Privacy & Protection Policy

COMPANY CONFIDENTIAL

Issue: 2

Revision: 2.0

Title: Data Privacy & Protection

Description: This document defines the Data Privacy and Protection policy at H2O and is approved by the Executive Committee.

1. TABLE OF CONTENTS

2. DEFINITIONS

Sources:

- *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);*
- *Schedule 1 of the Data Protection Act 2018;*
- *Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/*

Consent: 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 relating to him or her;

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;

Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Officer: see section 6.1.1.

***Data Recipient*:** a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Data Subject: the identified or identifiable living individual (identified natural person) to whom personal data relates.

General Data Protection Regulation ("GDPR"): regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Lawful basis: a lawful basis is a legal reason for having personal data and is required in order to legally process that data. It needs to be demonstrated that the data was obtained lawfully and will be processed in a manner that does not infringe the rights and freedoms of the individual whose data it is.

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 ("PD"): 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: 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.

Process, Processed, Processes and Processing: any operation, or set of operations, which is performed upon Personal Data, whether or not by automatic means. This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Sensitive Personal Data / Special Categories of Data: subset of personal data which includes but is not limited to personal data revealing or concerning (directly or indirectly) racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, 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.

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. INTRODUCTION

This policy is applicable to:

- H2O AM LLP
- H2O (Monaco) S.A.M.
- H2O Asia Pte. Ltd
- H2O AM Europe

Together "H2O".

This Data Privacy & Protection Policy (the "Policy") sets forth the expected behaviours of H2O in relation to the collection, use, retention, transfer, disclosure, and destruction of any Personal Data ("PD") belonging to an identifiable individual. H2O must comply with the data protection and data privacy laws that apply in their jurisdictions, as well as any data privacy laws of other jurisdictions which are applicable to their business and operations ("Data Protection Laws").

Violations of Data Protection Laws may result in civil or criminal liability, significant fines, and reputational harm for H2O and its employees who are responsible for processing data.

4. PURPOSE OF THE POLICY

H2O needs to gather and use certain information about individuals.

These individuals can include customers, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact. PD may only be collected when strictly necessary.

The purpose of this Policy is to formalize a global data protection framework for H2O and for each of its offices individually. Therefore, this Policy provides an overview of the principles generally contained in the Data Protection Laws, sets H2O's overarching approach to data protection and establishes minimum standards designed to assist its offices in implementing a data protection framework that is reasonably designed to prevent violations of Data Protection Laws. In countries outside the EU where Data Protection laws are typically less stringent or comprehensive than General Data Protection Regulation ("GDPR"), H2O has elected to implement the GDPR standards.

The Policy ensures H2O:

- Complies with data protection laws and regulations and follows good practice;
- Protects the rights of staff, customers and partners;
- Is open about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach.

5. POLICY SCOPE

5.1 TERRITORIAL SCOPE

Most organisations - including H2O - that process PD within the European Union ("EU") fall under the scope of the GDPR. However, the EU privacy rules now also can apply to Data Controllers and Data Processors outside the EU. The consequence of this expansion is that the GDPR applies to the processing of PD of Data Subjects who are in the EU by a Data Controller or a Data Processor not established[1] in the EU, where the processing activities are related to: (a) The offering of goods or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the EU; or (b) The monitoring of their behaviour as far as their behaviour takes place within the EU.

[1] While the notion of "main establishment" is defined in Article 4(16), the GDPR does not provide a definition of "establishment" for the purpose of Article 34 . However, Recital 225 clarifies that an "[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." *Source:* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

Where H2O (the "Data Controller") chooses to use a Data Processor located outside the EU and not subject to GDPR, it shall ensure by contract or other legal act that the Data Processor processes the data in accordance with the GDPR.

The Data Processor will have to ensure its processing remains lawful with regards to other obligations under EU or national law.

Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this Policy, the relevant national law must be adhered to.

5.2 INDIVIDUAL SCOPE

This Policy applies to:

- The head office and senior management of H2O;
- All branches of H2O;
- All staff and volunteers of H2O;
  All contractors, business contacts, suppliers, and other individuals working on behalf of H2O.

5.3 MATERIAL SCOPE

This Policy applies to all PD which H2O collects relating to identified or identifiable individuals ("Data Subjects"). This can include, but is not limited to, information regarding:

- Its employees, directors and company officers: Name, personal contact information, employment history, date of birth, national insurance number, personal banking details, emergency contact details, employment terms & conditions, educational history and qualifications, regulatory registrations, employment references, image rights authorisation, family circumstances, contact information, interview notes, any information provided by CV or relevant public social media or recruitment platform profiles, etc.

  Such information is usually collected at the time of hiring or appointment to office and updates may be needed through the years. At the time of hiring, the new employees are asked to sign the "Data Privacy Information Notice - Employee Agreement" that enables H2O to process its employees' PD;

- Its clients for the purpose of doing business with them: this includes, but is not limited to Know-Your-Customer / Anti-Money Laundering documentation (including, but not limited to, copies of passports, postal addresses, signatures and any other information relating to individuals);

- Its third party partners and service providers to allow them to provide services to H2O;

- Prospective clients;

- Visitors to H2O's website;
- Attendees at events organized by H2O or by its parent company Natixis Investment Managers.

This policy applies to all processing of PD in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about Data Subjects.

6. DATA PRIVACY AND PROTECTION RISKS

This policy helps to protect H2O from several real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all Data Subjects should be free to choose how H2O uses data relating to them.
- **Reputational damage.** For instance, H2O could suffer if Sensitive PD is unlawfully or inappropriately accessed.

7. POLICY

7.1 GOVERNANCE

7.1.1 OFFICE OF DATA PROTECTION

H2O takes responsibility for complying with the GDPR, at the highest management level and throughout the organisation.

To demonstrate our compliance to data privacy and data protection, and to enhance the effectiveness of our compliance efforts, H2O has established an Office of Data Protection (the Office). The Office operates with independence and is staffed by suitably skilled individuals granted all necessary authority. The Office includes the Data Protection Officer ("DPO"), the Compliance team, and a Data Protection Representative ("DPR") from the various H2O teams (i.e Client Services, HR, Middle Office, Risk etc.).

The duties of the DPO include:

- Informing and advising H2O and its employees who carry out processing pursuant to Data Protection Laws;
- Ensuring H2O employees trainings;
- Ensuring the alignment of this policy with data privacy and protection regulations or law;
- Providing guidance with regards to carrying out Data Protection Impact Assessments ("DPIAs");

- Investigating all reported incidents to confirm whether or not a PD breach has occurred and recording in H2O's data breach register any PD breaches, regardless whether H2O is required to notify to the relevant Data Protection Authorities ("DPAs") and the affected individuals;
- Acting as a point of contact for and cooperating with DPAs;
- Determining the need for, making, and keeping current notifications to one or more DPAs as a result of H2O's current or intended PD processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to individual's PD requests;
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this policy by anyone who:
    - Provides PD to H2O;
    - Receives PD from H2O;
- Ensuring that the processing of PD complies with the Data Protection Laws and especially the GDPR standards.

7.1.2 POLICY DISSEMINATION & ENFORCEMENT

H2O must ensure that all H2O employees responsible for the processing of PD are aware of and comply with the contents of this Policy.

All Third Parties engaged to process PD on their behalf (i.e. "Data Processors") are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to PD controlled by H2O.

7.1.3 DATA PROTECTION BY DESIGN AND BY DEFAULT

The GDPR requires putting into place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights: this is Data Protection by design and by default. Data protection by design is about considering data protection and privacy issues upfront in everything you do.

To ensure that all data privacy and protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

H2O must ensure that a DPIA is conducted for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the DPO for review and approval. H2O shall ensure that PD is automatically protected in any Information technology ("IT") system, service, product, and/or business practice, so that individuals should not have to take any specific action o protect their privacy.

Copies of the results of the DPIA must be kept by the DPO to demonstrate compliance with the Data Protection by Default and by Design requirement.

7.1.4 COMPLIANCE MONITORING

To confirm that an adequate level of compliance is being achieved by H2O in relation to this policy, an annual review will be undertaken by the DPO and the DPRs. The review will, as a minimum, assess:

- Compliance with this Policy in relation to the privacy and protection of PD including:
  - Raising awareness;
  - Training of employees;
- The effectiveness of data privacy and protection related operational practices, including:
  - Data Subjects' rights;
  - PD transfers;
  - PD incident management;
  - PD complaints handling;
- The level of understanding of data protection policies and privacy notices;
- The policy to ensure that it is up to date;
- The accuracy of PD being stored;
- The adequacy of procedures for redressing poor compliance and PD breaches.

The DPO will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified through the review will be reported and monitored by the DPO.

7.2 DATA PROTECTION PRINCIPLES

The Data Protection Act 2018 and the GDPR describe how organisations - including H2O - must collect, use, retain, disclose, and destroy PD.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, PD must be collected and used fairly, stored safely, not disclosed unlawfully, and destroyed appropriately. H2O has adopted the following principles as outlined in the Data Protection Act 2018[2] and the GDPR.[3]

1. *Lawfulness, fairness and transparency*

PD shall be processed lawfully, fairly and in a transparent manner in relation to individuals. H2O must tell the Data Subject what processing will occur, the processing must match the description

[2]Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted?_ga=2.42074860.892985804.1566984390-166940600.1561715912

[3] Regulation (EU) 2016/679 (*General Data Protection Regulation),* Article 5.

given to the individual, and it must be for one of the purposes specified in the applicable data privacy and protection regulation.

For processing of PD to be lawful, a specific ground for the processing must be identified: see section 7.4.1.. The GDPR displays six lawful bases that legitimise PD processing: consent from the Data Subject; contractual relation; legitimate interest; legal obligation; vital interest; and public task. H2O shall process PD only if one of these lawful bases is applicable.

Fairness means that H2O shall ensure to only handle PD in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

Transparent processing is about being clear, open and honest with individuals from the start about who H2O is, and how and why H2O uses their PD.

2. *Data minimisation*

PD shall be collected for specified, explicit, and lawful purposes and not further processed in a manner that is incompatible with those purposes. Therefore, H2O must specify what the PD collected will be used for and limit the processing of that PD to only what is necessary to meet the specified purpose.

PD shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. H2O must not store any PD beyond what is strictly required.

3. *Accuracy*

PD shall be accurate and kept up to date. H2O must have processes in place for identifying and addressing out-of-date, incorrect, and redundant PD.

4. *Storage limitation*

PD shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the PD is processed. H2O must, wherever possible, store PD in a way that limits or prevents identification of the Data Subjects.

5. *Integrity & confidentiality*

PD shall be processed in a manner that ensures appropriate security of the PD, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. H2O must use appropriate technical and organisational measures to ensure the integrity and confidentiality of PD is maintained at al times.

6. *Accountability*

The DPO shall be responsible for, and be able to demonstrate compliance with the above principles. H2O must be able to demonstrate that the principles above are met for all PD for which it is responsible.

7.3 DATA COLLECTION

H2O will obtain PD only by lawful and fair means.

7.3.1 CONSENT TO ALLOW DATA COLLECTION

Where a need exists and requires the Consent of a Data Subject prior to the collection, use or disclosure of their PD, H2O is committed to seeking such Consent.

The DPO will ensure that mechanisms are in place to obtain and document Data Subjects' Consent for the collection, processing, and/or transfer of their PD.

The request for Consent will be presented to the Data Subject:

- in a manner which is clearly distinguishable from any other matters and;
- is made in an intelligible and easily accessible form, and uses clear and plain language.

The Consent must be freely given and not based on a condition of a contract. H2O will allow consent to be withdrawn at any time via notification from the individual.

Consent will be deemed given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of PD relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

The Data Subject shall have the right to withdraw his or her consent at any time, but the withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.

7.3.2 DATA COLLECTION OUTSIDE OF CONSENT

H2O is able to collect PD out of the Data Subject's consent when one of the following lawful bases is applicable: contractual relation; legitimate interest; legal obligation; vital interest; and public task.

For instance, in the course of its activities, H2O shall collect PD:

- to provide its services and fulfil its contractual obligations with clients or third parties;
- for legal and regulatory compliance purposes. This includes responses to governmental, regulatory or law enforcement agency requests as required. For instance H2O shall collect PD information to perform identity checks and fraud checks to ensure compliance with its Anti-Money Laundering obligations;
- for H2O's legitimate business interest in :
    a. Ensuring the quality of the products and services we provide;
    b. Collecting information for marketing purposes;

c. Communicating with Clients of the emails from Clients / Prospective clients on the basis of its legitimate business interest;
d. The physical security of our premises;
e. Statistical analysis;

In these cases and more generally when a lawful basis exists apart from Consent, Data Collection can be done from other persons or bodies than the Data Subject if they can provide they have the authorization to disclose those data.

If PD is collected from someone other than the Data Subject, then the Data Subject must be informed of the collection. An exception to this justification can occur only if:

- the Data Subject has received the required information by other means; or
- the information must remain confidential due to a professional secrecy obligation; or
- a national law expressly provides for collection, processing or transfer of PD.

Notification to the Data Subject should be sent promptly and in any case by the earliest of:

- one calendar month from the first collection or recording of PD; or
- at the time of first communication, if the PD is used for communicating with the Data Subject; or
- at the time of disclosure, if the PD is disclosed to another recipient.

7.3.2 DATA COLLECTION ON H2O WEBSITE

H2O shall publish a privacy notice on its website to inform all visitors of its commitments to ensure confidentiality of PD and to comply with Data Protection Laws and especially with the GDPR.

H2O's privacy notice is displayed in Appendix C.

7.4 DATA USE

7.4.1 DATA PROCESSING

H2O, as a Data Controller, must exercise control over the processing and carry data protection responsibility for it.

H2O processes PD of its clients, prospective clients, employees, and others for the following broad purposes (but not limited to):

- The general running and business administration of H2O;
- Employee / staff / partner management/ Recruitment;
- Management of clients and prospective clients who are individuals;
- Compliance with its legal and regulatory obligations;

- To offer/provide/ensure quality of its investment services to clients and prospective clients;
- The performance of contracts;
- Fraud prevention;
- Network and information security;
- Direct marketing;

H2O acknowledges the requirement for a valid lawful basis in order to process PD. If no lawful basis applies to processing, it will be unlawful and in breach of the first principle (see section 7.2.1).

The processing of Data Subjects' PD should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

H2O will process PD in accordance with all applicable laws and regulations, and applicable contractual obligations. More specifically, H2O will not process PD unless it finds that there is lawful basis to do so, in accordance with the principles of the GDPR:

- The Data Subject has given consent to the processing of their PD for one or more specific purposes (see section 7.3.1);
- Processing is necessary[4] for the performance of a contract to which the Data Subject is a party to or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with a legal or regulatory obligation;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject;
- Processing is necessary to protect an individual's vital interests;
- Processing is necessary for public task.

H2O considers the perspectives and expectations of Data Subjects in the processing of their PD and avoids any behaviour that would be contrary to their expectations or that could potentially harm the rights and freedom of an individual or group of individuals.

Before starting any new or further processing of PD, H2O must verify whether additional Consent must be obtained from the Data Subject and/or whether an updated privacy notice must be provided to the relevant Data Subject.

[4] This does not mean that processing has to be absolutely essential. However, it must be more than just useful and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data. *Source* : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

When no other lawful basis can be established to process an individual's PD, or when the processing is not deemed necessary, explicit Consent must be obtained from the Data Subject.

7.4.2 SPECIAL CATEGORIES OF DATA

Special Categories of Data (Sensitive Data) need more protection. For instance, information about an individual's: race, ethnic origin, age, gender, religious or philosophical beliefs, politics, genetics, biometrics, health, sex life or sex orientation.

The lawful process of Special Categories of Data implies:

- a lawful basis under Article 6 of the GDPR in exactly the same way as for any other PD and;
- a specific condition to be satisfied under Article 9 of the GDPR.

Therefore H2O shall process Special Categories of Data only when the Data Subject gives its consent to the processing (Article 6 of the GDPR) which must be explicit (Article 9 of the GDPR).

H2O shall collect, use and store its employees' Sensitive Data only with their prior explicit consent. Their consent shall be considered as explicit if they have signed the H2O Data Privacy Information Notice.

In any situation where Special Categories of Data are to be processed, prior approval must be obtained from the DPO and the basis for the processing clearly recorded with the PD in question.

7.4.3 DATA QUALITY

H2O will adopt all necessary measures to ensure that the PD it collects and processes is complete and accurate in the first instances, and is updated to reflect the current situation of the individual.

These measures include:

- Correcting PD as required, even if the Data Subject has not requested rectification;
- Keeping PD only for the required period of use in accordance with the Data Retention Schedule;
- PD is appropriately removed or erased if it is violation of the Data Protection principles or if the PD is no longer required;
- Restriction, rather than deletion of PD, insofar as:
    - A law prohibits erasure;
    - Erasure would impair legitimate interests of the individual;
    - The Data Subject disputes that their PD is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

7.5 DATA RETENTION

To ensure fair processing, PD will not be retained by H2O for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

Attached as Appendix A which sets out the length of time in which PD needs to be retained. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All PD should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

7.6 DATA PROTECTION

H2O adopts physical, technical, and organisational measures to ensure the security of PD. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical, natural or electronic environment.

The security measures adopted by H2O are set out in H2O's IT Security and Cyber Security policies. A summary of the related security measures is below:

- Prevent unauthorised persons from gaining access to data processing systems in which PD is processed;
- Prevent persons entitled to use a data processing system from accessing PD beyond their needs and authorisations;
- Ensure that PD in the course of electronic transmission during transport cannot be read, copied, modified, or removed without authorisation;
- Ensure that PD is protected against undesired destruction or loss;
- Ensure that PD is not kept longer than necessary.

7.7 INDIVIDUALS' RIGHTS

The DPO will establish a system to enable and facilitate the exercise of the Data Subjects' rights with respect to their PD. Specifically:

- Information access (The right of access and to be informed);
- Objection to processing (The right to object);
- Objection to automated decision-making and profiling (Rights in relation to automated decision-making and profiling);
- Restriction of processing (The right to restrict processing);
- Data portability (The right to data portability);
- Data rectification (The right to rectification);
- Data erasure (The right to erasure).

A detailed explanation of these rights is listed in Appendix B of the Policy.

If a Data Subject makes a request relating to any of the rights listed above, H2O will consider each such request in accordance with all applicable data protection laws and regulations.

Data Subjects are entitled to obtain, based upon a request made in writing to the DPO and upon successful verification of their identity, the following information about their own PD:

- The purposes of the collection, processing, use and storage of their PD;
- The source(s) of the PD, if it was not obtained from the individual;
- The categories of PD stored for the individual;
- The recipients or categories of recipients to whom the PD has been or may be transmitted, along with the location of those recipients;
- The envisaged period of storage for the PD or the rationale for determining the storage period;
- The use of any automated decision-making, including profiling.

7.8 LAW ENFORCEMENT REQUESTS & DISCLOSURES

H2O is permitted to disclose PD without the consent of the Data Subject only for the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty;
- By the order of a court or by any rule of law.

If H2O receives a request from a court or any regulatory or law enforcement authority for PD relating to a Data Subject, you must notify the DPO or a DPR who will provide guidance and assistance.

7.9 DATA PRIVACY & PROTECTION TRAINING

All H2O employees that have access to PD will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, H2O will provide regular data privacy and protection training and procedural guidance for its employees.

7.10 DATA TRANSFERS

H2O may transfer PD to internal or Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant individuals. Where transfers need to be made to countries lacking an adequate level of legal protection, they must be made in compliance with the approved transfer procedures.

H2O may only transfer PD where one of the scenarios below applies:

- The Data Subject has given consent to the proposed transfer;
- The transfer is necessary for the performance of a contract with the Data Subject;
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the Data Subject;

- The transfer is legally required on important public interest grounds;
- The transfer is necessary for the establishment, exercise, or defence of a legal claims;
- The transfer is necessary in order to protect the vital interests of the Data Subject.

8. COMPLAINTS HANDLING

Data Subjects with a complaint about the processing of their PD should put forward the matter in writing to the DPO. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Subject will be informed of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the DPO, then the Data Subject may seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

8.1 BREACH REPORTING

Any Data Subject who suspects that a PD breach has occurred due to the theft or exposure of PD must immediately notify the DPO providing a description of what occurred. Notification of the incident can be made via e-mail compliance@h2o-am.com, or by calling +44 2072 920 313.

The DPO will investigate all reported incidents to confirm whether or not a PD breach has occurred. All incidents shall be reported in H2O's Data Breach Register.

If a PD breach is confirmed then the DPO will follow the authorised procedure based on the significance of the breach.

Severe PD breaches:

PD Breaches that may present a risk to the individual's rights and freedoms are considered as severe. In case of a severe PD breach:

- H2O will engage counsel and determine an appropriate response to the PD breach;
- H2O will report it to the DPAs within 72 hours of becoming aware of the breach.

9. RELATED DOCUMENTS

- Data Privacy Information Notice - Employee Agreement
- Privacy Notice - Website & Investors (Appendix C)
- Information Security Policy
- Individual's Request Handling Procedure
- Personal Data Retention Schedule (Appendix A)
- Data Breach register
- Data Protection Impact Assessment Template

10. APPENDICES

Appendix A - Personal Data Retention Schedule

Appendix B - Individual Rights

Appendix C - Privacy notice - Website & Investors

Appendix A - Personal Data Retention Schedule

PURPOSE OF THIS DOCUMENT

A vital part of H2O's Data Privacy and Protection Policy (the Policy) and practice is that personal data (PD) is retained for the appropriate period of time. The Policy states that H2O must:

- *…not retain PD longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.*

This document outlines the retention period for PD held by H2O and gives an indication of the kind of PD which needs to be retained for longer than is normally required.

11. DEFINITIONS

"Client"	
"CV, education data"	
"Economic & financial data"	
"Employee"	An individual who works part-time or full-time for H2O AM LLP or one of it's affiliates under a contract of employment (oral or written, express or implied)
"Health data"	Personal Data relating to the individuals' health including DNA, blood data and other. This is a Special Category of Data.
"Identification data"	
"Job candidates"	
"Location data"	
"Offenses, convictions or security measures"	Personal Data relating to the individuals' criminal history or other security concerns. This is a Special Category of Data.
"Personal life data"	
"Personal preferences data"	
"Professional life data"	
"Racial or ethnic origin data"	Personal Data relating to the race or ethnicity of the individuals. This is a Special Category of Data.
"Religious or philosophical beliefs"	Personal Data relating to the religious, philosophical or other beliefs of the individuals. This is a Special Category of Data.
"Sex life or sexual orientation data"	Personal Data relating to the sexual orientation and preferences of the individuals. This is a Special Category of Data.
"Unique national identification number"	

Section	Data Subject	Categories of data (*italics = Sensitive data*)	Retention Timescale (years)	Reason(s) for Processing[5]
i.e: Payroll	*Client*	*Bank details*	*Current Year + 3*	*Legal*
HR	Employee	Identification data	End of employment + 6	BA, IF, LR
		CV, Education data	End of employment + 6	BA, IF, LR
		Personal life data	End of employment + 6	BA, IF
		Professional life data	End of employment + 6	BA, IF
		Economic & financial data	End of employment + 6	BA, IF
		Location data	End of employment +2	BA
		Racial or ethnic origin data	End of employment + 6	IF
		Religious or philosophical beliefs	End of employment + 6	IF
		Offenses, convictions or security measures	End of employment + 6	BA, IF, LR
		Health data	End of employment + 6	IF
		Data on sex life or sexual orientation	End of employment + 6	IF
		Unique national identification number	End of employment + 6	BA, IF, LR
		Personal preferences data	End of employment + 1	BA
	Job Candidates	Identification data	Last contact + 1	BA, IF, R
		CV, Education data	Last contact + 1	BA, IF, R
		Personal life data	Last contact + 1	BA, IF, R
		Professional life data	Last contact + 1	BA, IF, R
Finance/ Accounts	Employee	Identification data	End of employment + 6	BA, IF, CO
		Economic & financial data	End of employment + 6	BA, IF
		Unique national identification number	End of employment + 6	BA, CO
	Client	Identification data	End of dealings + 6	BA, IF, LR, CO
		Economic & financial data	End of dealings + 6	BA, IF, LR, CO
		Unique national identification number	End of dealings + 6	BA, LR, CO
	Contact persons and/or legal reps of clients	Identification data	End of dealings + 6	BA, IF, LR, CO
		Economic & financial data	End of dealings + 6	BA, IF, LR, CO
		Unique national identification number	End of dealings + 6	BA, LR, CO
IT	Employee	Identification data	End of employment + 6	BA, IF
		Personal preferences data	End of employment + 1	BA
	Client	Identification data	End of dealings + 6	BA, IF, LR
Middle Office	Employee	Identification data	End of employment + 6	BA, IF

[5] CO = Contractual Obligations; BA = Internal Business Admin & Record Keeping; LR = Legal & Regulatory Compliance; IF = Identification & Fraud Protection, R = Recruitment, CU = Client Updates & Communication

Section	Data Subject	Categories of data (*italics = Sensitive data*)	Retention Timescale (years)	Reason(s) for Processing[5]
	Client	Identification data	End of dealings + 6	BA, IF, LR, CO
		Economic & financial data	End of dealings + 6	IF, LR, CO
	Contact persons and/or legal reps of clients	Identification data	End of dealings + 6	BA, LR, CO
Client Services	Employee	Identification data	End of employment + 6	BA, IF
		Professional life data	End of employment + 6	BA, CU
	Client	Identification data	End of dealings + 6	BA, IF
		Economic & financial data	End of dealings + 6	BA, IF
	Contact persons and/or legal reps of clients	Identification data	End of dealings + 6	BA, IF
Risk	Employee	Identification data	End of employment + 6	BA, IF
	Client	Identification data	End of dealings + 6	
	Contact persons and/or legal reps of clients	Identification data	End of dealings + 6	
Compliance	Employee	Identification data	End of employment + 6	
		CV, Education data	End of employment + 6	
	Client	Identification data	End of dealings + 6	
		Offenses, convictions or security measures	End of dealings + 6	
	Contact persons and/or legal reps of clients	Identification data	End of dealings + 6	
		Offenses, convictions or security measures	End of dealings + 6	

Appendix B - Individual Rights[6]

1) Right to be informed

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.
Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about, namely:

- The name and contact details of H2O;
- The name and contact details of H2O's representative;
- The contact details of H2O's DPO;
- The purposes of the processing;
- The lawful basis for the processing
- The categories of Personal data obtained;
- The recipients or categories of recipients of the Personal Data;
- The details of transfers of the personal Data to any third countries or international organisations; -

The retention periods for the Personal Data;

- The rights available to individuals in respect of the processing -

The right to withdraw consent;

- The right to lodge a complaint with a supervisory authority; -

The source of the Personal Data;

- The details of whether individuals are under a statutory or contractual obligation to provide the Personal Data;
- The details of the existence of automated decision-making, including profiling.

2) Right of access

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data.
An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).
In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient H2O disclosed the Personal Data to;
- H2O's retention period for storing the personal data or, where this is not possible, H2O's criteria for determining how long H2O will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;

[6] Source: Information Commissioner's Office website: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/*

- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual; - the existence of automated decision-making (including profiling); and
- the safeguards H2O provides if it transfers personal data to a third country or international organisation.

3) Right to rectification

Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed - although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

4) Right to erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.
Individuals have the right to have their Personal Data erased if:

- the Personal Data is no longer necessary for the purpose which H2O originally collected or processed it for;
- H2O is relying on consent as its lawful basis for holding the data, and the individual withdraws their consent;
- H2O is relying on legitimate interests as its basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; - H2O is processing the Personal Data for direct marketing purposes and the individual objects to that processing;
- H2O has processed the Personal Data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- H2O has to do it to comply with a legal obligation; or
- H2O has processed the Personal Data to offer information society services to a child.

5) Right to restrict processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.
Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their Personal Data and H2O is verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- H2O no longer needs the Personal Data but the individual needs H2O to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to H2O processing their data under Article 21(1), and H2O is considering whether its legitimate grounds override those of the individual.

6) Right to data portability

The right to data portability gives individuals the right to receive Personal Data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.
The right to data portability only applies when:

- H2O's lawful basis for processing this information is consent **or** for the performance of a contract; and
- H2O is carrying out the processing by automated means (i.e. excluding paper files).

7) Right to object

Article 21 of the GDPR gives individuals the right to object to the processing of their Personal Data. This effectively allows individuals to ask H2O to stop processing their Personal Data.
Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.
Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in H2O; or
- H2O's legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

8) Rights related to automated decision-making including profiling

Automated individual decision-making is a decision made by automated means without any human involvement.
Examples of this include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, although it often will do. Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances.
H2O can **only** carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

If H2O is using special category personal data it can **only** carry out processing described in Article 22(1) if:

- H2O has the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest.

Appendix C - Privacy notice - Website & Investors

Appendix C - Privacy Notice - Website & Investors WEB SITE VERSION.pdf