



H2O
Asset Management

DO NOT COPY

H2O AM LLP

Data Privacy & Protection Policy

PROPERTY OF H2O

1 CONTENTS

1	Contents	2
2	Introduction.....	4
3	Policy scope	4
3.1	Data privacy and protection risks	5
4	Policy	5
4.1	Governance.....	5
4.1.1	Office of data protection	5
4.1.2	Policy Dissemination & Enforcement	6
4.1.3	Data Protection by Design	6
4.1.4	Compliance Monitoring	6
4.2	Data Protection Principles	7
4.3	Data Collection.....	8
4.4	Data Use.....	8
4.4.1	Data Processing	8
4.4.2	Special Categories of Data.....	9
4.4.3	Data Quality.....	9
4.5	Data Retention.....	10
4.6	Data Protection.....	10
4.7	individuals' Requests	10
4.8	Law Enforcement Requests & Disclosures.....	11
4.9	Data Privacy & Protection Training.....	11
4.10	Data Transfers.....	11
4.10.1	Transfers between H2O Entities	Error! Bookmark not defined.
4.10.2	Transfers to Third Parties.....	Error! Bookmark not defined.
4.11	Complaints Handling.....	12
4.12	Breach Reporting	12
5	Related Documents	12

PROPERTY OF H2O AM LLP - DO NOT COPY

2 INTRODUCTION

This policy is applicable to:

- H2O AM LLP
- Arctic Blue Capital Ltd.
- H2O (Monaco) S.A.M.

Together “H2O”.

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.

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.

PD is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

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

3 POLICY 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, suppliers, and other people working on behalf of H2O

It applies to all PD H2O holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 or the General Data Protection Regulation (GDPR). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

- Any other information relating to individuals

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 individuals.

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.

3.1 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 individuals should be free to choose how H2O uses data relating to them.
- **Reputational damage.** For instance, H2O could suffer if sensitive data is unlawfully or inappropriately accessed.

4 POLICY

4.1 GOVERNANCE

4.1.1 OFFICE OF DATA PROTECTION

To demonstrate our commitment to data privacy and protection, and to enhance the effectiveness of our compliance efforts, H2O has established an *Office of Data Protection*. 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.).

Jean Noel Alba has been nominated as the DPO of H2O. He has direct access to the H2O Board of Directors and is the ideal selection for the DPO role. The duties of the DPO include:

- Informing and advising H2O and its employees who carry out processing pursuant to data privacy and protection regulations or national law
- 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)
- Acting as a point of contact for and cooperating with Data Protection Authorities (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
 - Has access o PD collected or processed by H2O

4.1.2 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 their 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.

4.1.3 DATA PROTECTION BY DESIGN

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 Data Protection Impact Assessment (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. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will assist in assessing the impact of any new technology uses on the security of PD.

4.1.4 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:
 - Individuals' 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.

4.2 DATA PROTECTION PRINCIPLES

The Data Protection Act 1998 and the GDPR describes 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 1998¹ and the GDPR.²

1. *Lawfulness, fairness and transparency*

PD shall be processed lawfully, fairly and in a transparent manner. H2O must tell the individual what processing will occur, the processing must match the description given to the individual, and it must be for one of the purposes specified in the applicable data privacy and protection regulation.

2. *Purpose limitation*

PD shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. 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.

3. *Data minimisation*

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.

4. *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.

¹ *Data Protection Act 1998*, UK, Schedule 1, Part 1, <https://www.legislation.gov.uk/ukpga/1998/29/contents> (Accessed: 01/03/2018)

² *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 5.

5. Storage limitation

PD shall be kept in a form which permits identification of individuals 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 individual.

6. 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 all times.

7. Accountability

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

4.3 DATA COLLECTION

H2O will obtain PD only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual 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 individuals' consent for the collection, processing, and/or transfer of their PD.

The request for consent will be presented in a manner which is clearly distinguishable from any other matters, 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.

4.4 DATA USE

4.4.1 DATA PROCESSING

H2O uses the PD of its clients, employees, and others for the following broad purposes:

- The general running and business administration of H2O
- Employee / staff / partner management
- Management of clients and potential clients who are individuals

The use of individuals' 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 at least one of the following requirements is met:

- The individual has given consent to the processing of their PD for one or more specific purposes
- Processing is necessary for the performance of a contract to which the individual is a party to or in order to take steps at the request of the individual prior to entering into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary in order to protect the vital interests of the individual or another natural person

4.4.2 SPECIAL CATEGORIES OF DATA

H2O will only process Special Categories of data (sensitive data) where the individual expressly consents to its processing or where one of the following applies:

- The processing relates to PD which has already been made public by the individual;
- The processing is necessary for the establishment, exercise, or defence of legal claims;
- The processing is specifically authorised or required by law;
- The processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent;
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or concerning health.

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.

4.4.3 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 individual 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 individual disputes that their PD is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

4.5 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.

4.6 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 or natural 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 are 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.

4.7 INDIVIDUALS' REQUESTS

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

- Information access
- Objection to processing
- Objection to automated decision-making and profiling
- Restriction of processing
- Data portability
- Data rectification
- Data erasure

If an individual 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.

H2O AM LLP, Arctic Blue Capital Ltd., H2O (Monaco) S.A.M. – Data Privacy & Protection Policy: March 2018 Version 1.1

Individuals 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

4.8 LAW ENFORCEMENT REQUESTS & DISCLOSURES

H2O is permitted to disclose PD without the consent of the individual 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 an individual, you must notify the DPO or a DPR who will provide guidance and assistance.

4.9 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.

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

4.11 COMPLAINTS HANDLING

Individuals 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 Individual 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 individual and the DPO, then the individual may seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

4.12 BREACH REPORTING

Any individual 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. If a PD breach is confirmed then the DPO will follow the authorised procedure based on the significance of the breach. For severe PD breaches, H2O will engage counsel and determine an appropriate response to the PD breach.

5 RELATED DOCUMENTS

- Internet Privacy Notice template
- Information Security Policy
- Individual's Request Handling Procedure
- Personal Data Retention Schedule

6 APPENDIX

Appendix A – Personal Data Retention Schedule

