The General Data Protection Regulations 2018

Policy

Introduction

Hydrobolt Limited hold Personal Data about our employees, clients, suppliers and other individuals for a variety of business purposes. These business purposes are set out in the appropriate Data Protection Policy Statement & Privacy Statement that are sent to Data Subjects as appropriate.

This policy sets out how we seek to protect Personal Data and ensure that employees understand the rules governing their use of Personal Data to which they have access in the course of their work.

Personal Data Protection Principles

We will process Personal Data in compliance with the following data protection principles:

- Used fairly and lawfully and in a transparent manner
- Used for legitimate, specifically stated purposes
- Used in a way that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and where necessary kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed.
- Handled according to individual's data protection rights
- Kept safe and secure, using appropriate technological and organisational measures to protect against unauthorised or unlawful processing and accidental loss
- Not transferred outside the EEA without adequate protection

Definitions

General Data Protection Regulation (GDPR)	The General Data Protection Regulation ((EU) 2016/679).
Personal Data	Information identifying an individual, such as job applicant, current or former employee, agency, contractor and other staff, client, supplier and marketing contact, or information relating to an individual that we can identify (directly or indirectly) from that information alone or in combination with other identifiers we possess or can reasonably access. Personal Data excludes anonymous Personal Data or Personal Data that has had the identity of an individual permanently removed. Personal Data we gather may include factual information, such as individuals' name, contact details, email address, date of birth, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV or an opinion about that person's actions or behaviour.
Data Protection Policy Statement & Privacy Statement	Separate documents setting out information that may be provided to Data Subjects when the Company collects information about them, including the purposes for which their Personal Data may be used. These documents may take the form of general privacy statements applicable to a specific group of individuals or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.
Sensitive Personal Data	Information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, sexual orientation, biometric or genetic Personal Data, and information relating to criminal offences and convictions.

Scope

This policy applies to all employees. You must be familiar with this policy and comply with its terms. This policy is not contractual.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. You will be advised of any amendments to this policy and the policy can be found via the HR department.

Who is responsible for this policy?

Data Controller (the Business Unit Committee) has overall responsibility for the day-to-day implementation of this policy.

Responsibilities of the Data Controller (the Business Unit Committee):

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to make requests in respect of their Personal Data under this policy, including to know which data is being held on them by Hydrobolt Limited.
- Checking and approving with third parties that handle the Company's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the Company is considering using to store or process data

Responsibilities of our Employees

- Provide accurate personal data in the most efficient, secure, and effective manner possible, and for purposes as described at the point of collection, or for purposes which are legally permitted
- Securely destroy data which is no longer needed
- Take appropriate technical and organisational security measures to safeguard information
- Ensure information is not transferred abroad without suitable safeguards

Our Procedures

Fair and lawful processing

We must process Personal Data fairly, lawfully and transparently, for specified purposes and in accordance with Data Subjects' rights.

The GDPR allows processing for the following specific purposes:

- the Data Subject has given his or her consent;
- the processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations.;
- to protect the Data Subject's vital interests; or
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

The legal ground(s) being relied on for each processing activity will be set out in the relevant Privacy Notice.

Consent

The Company must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR. This includes consent.

A Data Subject consents to the processing of their Personal Data or Sensitive 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. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

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 of processing, explicit consent is usually required for processing Sensitive Personal Data and for cross border Personal Data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of Sensitive Personal Data.

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

Accuracy and Relevance

We will ensure that any Personal Data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process Personal Data obtained for one purpose for any unconnected purpose unless the Data Subject has agreed to this or would otherwise reasonably expect this.

We will also ensure that Personal Data is, where necessary, kept up to date. Data Subjects may ask that we correct inaccurate Personal Data relating to them. In such circumstances, we must correct or delete this Personal Data without undue delay.

All employees must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the relevant Data Controller (the Business Unit Committee).

Employees are responsible for only processing Personal Data when performing their job duties requires it. Employees should not process Personal Data for any reason unrelated to their job duties.

Employees are responsible for only collecting Personal Data that they require for their job duties and should not collect excessive Personal Data. Employees should ensure any Personal Data collected is adequate and relevant for the intended purposes.

Your Personal Data

You must take reasonable steps to ensure that Personal Data we hold about you is accurate, complete and updated as required. For example, if your personal circumstances change, please inform the Data Controller (the Business Unit Committee) so they can update your records.

Data Security

You must keep Personal Data secure against loss or misuse. Where other organisations process Personal Data as a service on our behalf, the relevant Data Controller (the Business Unit Committee) will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing Personal Data Securely

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks.

We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

Employees are responsible for protecting the Personal Data we hold. Employees are responsible for implementing reasonable and appropriate security measures against unlawful or unauthorised

processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Employees must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

In particular:

- In cases when Personal Data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed Personal Data should be shredded when it is no longer needed
- Personal Data stored on a computer should be protected by strong passwords and/or user access restrictions that are changed regularly.
- Personal Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The relevant Data Controller (the Business Unit Committee) must approve any cloud used to store Personal Data
- Servers containing Data must be kept in a secure location, away from general office space
- Personal Data should be regularly backed up in line with the Company's backup procedures
- Personal Data should never be saved directly to mobile devices such as laptops, tablets or smartphones, unless specified by your role/position in the organisation. All Personal Data must be encrypted, where and when practical. Please consult your IT team for best practices, questions, or concerns.
- All servers containing Sensitive Personal Data must be approved and protected by security software and strong firewall, and will be subject to audit from time to time.

Data Retention

We must retain Data for no longer than is necessary for the purposes for which the Personal Data is processed. What is necessary will depend on the circumstances of each case, taking into account the reasons that the Personal Data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Employees are responsible for taking all reasonable steps to destroy or erase from our systems all Personal Data that the Company no longer requires in accordance with our Personal Data retention guidelines. This includes requiring third parties to delete such Personal Data where applicable.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Privacy by Design and Default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Controller (the Business Unit Committee) will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the Data Subject, privacy settings will be set to the most private by default.

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.

Employees must 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 along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

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

- they have a need to know the information for the purposes of providing the contracted services;
- 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;
- the third party has agreed to comply with the required Personal Data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained.

International Personal Data Transfers

The GDPR restricts Personal Data transfers to countries outside the EEA in order to ensure that the level of Personal Data protection afforded to individuals by the GDPR is not undermined. Personal Data is transferred across borders when it is transmitted, sent, viewed or accessed in or to a different country.

No Personal Data may be transferred outside of the EEA without first discussing it with the Data Controller (the Business Unit Committee) and one of the following conditions must always apply:

- 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;

- appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Human Resources department;
- specific consent from the Data Subject has been obtained prior to transferring their Personal Data outside the EEA.
- 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 where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

Data Audit and Register

Regular data audits to manage and mitigate risks will form the data register. This contains information on what Personal Data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Employees are responsible for keeping and maintaining accurate 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, 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.

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate any failures and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures within 72 hours.
- In certain circumstances, notify any Data Subjects who may be affected by a Personal Data Breach

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 person or team designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach.

Examples of Personal Data Breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor

- Sending Personal Data to an incorrect recipient
- Computing devices containing Personal Data being lost or stolen
- Alteration of Personal Data without permission
- Loss of availability of Personal Data

Monitoring

Everyone must observe this policy. The Data Controller (the Business Unit Committee) has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. Subject to certain exemptions, these include rights to:

- withdraw consent to processing at any time;
- receive certain information about our processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate Personal Data or to complete incomplete Personal Data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- 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.

Employees are responsible for verifying the identity of an individual requesting Personal Data under any of the rights listed above (and must not allow third parties to persuade them into disclosing Personal Data without proper authorisation).

If you receive a request, you should refer that request immediately to the Data Controller (the Business Unit Committee) we may ask you to help us comply with those requests.

All employees should contact the Data Controller (the Business Unit Committee) if you would like to make any of the requests listed above.

Data Protection Policy Statement & Privacy Statement

The GDPR requires us 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 which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we will provide the Data Subject with the following information:

- What information is being collected
- Who is collecting the information
- How the information is collected
- Why the information is being collected
- How the information will be used
- Who the information will be shared with
- Identity and contact details of any data controllers
- Details of transfers to any third country and safeguards
- Retention period

Significances of Failing to Comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures and/or pursuant to applicable local/national/international laws.

If you have any questions or concerns about anything in this policy, do not hesitate to contact HR at the Company.

Jamie Simpson
Managing Director