Data Retention Policy (GDPR Compliant)

Data controller: Habasit (UK) Ltd
Habegger House
Gannex Park
Dewsbury Road
Elland
HX5 9AF

1 INTRODUCTION

1.1 Habasit (UK) Ltd ("we", "our", "us" or "the Company") must comply with our obligations under data protection laws (including the GDPR and the Data Protection Act 2018) whenever we Process Personal Data relating to our employees, workers, customers and suppliers and any other individuals we interact with.

1.2 This includes the obligation not to Process any Personal Data which permits the identification of Data Subjects for any longer than is necessary and the purpose of this policy is to assist us to comply with that obligation. This policy should be read alongside the Data Retention Matrix which is appended at Schedule 1 to this policy and which provides guideline data retention periods for various different types of Personal Data we hold.

1.3 Compliance with this policy will also assist us to comply with our 'data minimisation' and accuracy obligations under data protection laws which require us to ensure that we do not retain Personal Data which is irrelevant, excessive, inaccurate or out of date.

1.4 A failure to comply with data protection laws could result in enforcement action against the Company, which may include substantial fines of up to €20 million or 4% of total worldwide annual turnover (whichever is higher), significant reputational damage and potential legal claims from individuals. It can also have personal consequences for individuals in certain circumstances i.e. criminal fines/imprisonment or director disqualification.

1.5 Compliance with this policy will also assist in reducing the Company's information storage costs and the burden of responding to requests made by Data Subjects under data protection laws such as access and erasure requests.

1.6 We are also required under data protection laws to inform Data Subjects about how long we will retain their Personal Data in our privacy notices.

1.7 This policy is for internal-use only and cannot be shared with third parties, customers or regulators without prior authorisation from our Data Protection Manager.

1.8 For definitions of capitalised terms used in this policy, please refer to the Definitions appended at Schedule 2 to this policy.

2 SCOPE

2.1 This policy and the Data Retention Matrix specify the retention and destruction requirements that apply to all Information Assets that are held by the Company and which contain Personal Data, regardless of the form they take i.e. paper, electronic records, CD/DVDs etc. This includes, but is not limited to, letters, emails, attendance notes, financial information (such as statements or invoices), reports, legal documents (such as contracts and deeds) and photographs that contain or constitute Personal Data.

3 RESPONSIBILITY

3.1 Compliance with this policy is overseen by the Data Protection Manager (contactable via phone on 0333 207 6570 or email at caroline.hirst@habasit.com). The Data Protection Manager will retain a record of the training provided to personnel to ensure that they understand the Company's data retention and destruction obligations, their own responsibilities and the internal processes they need to follow.

3.2 Information Asset owners are responsible for ensuring that all Information Assets containing Personal Data that are within their control are retained and destroyed in accordance with this policy and the Data Retention Matrix. They must implement measures to ensure that they can identify when a retention period is due to expire, so that they can carry out a review and determine whether the Personal Data should be deleted or destroyed. In addition, Information Asset owners should carry out periodic reviews at least annually of the Personal Data contained in the Information Assets that are within their control (even if that Personal Data is not covered by a retention period contained in the Data Retention Matrix), to determine whether it is being retained and destroyed in accordance with this policy. Information Asset owners may delegate routine tasks, where appropriate.

3.3 This policy applies to all Company personnel ("you" or "your") and it sets out what we expect from you to assist the Company to comply with its data retention and destruction obligations under data protection laws. All Company personnel play a vital role and you must read and ensure that you fully understand and comply with this policy in relation to all Personal Data which you Process on our behalf and you must attend all related training provided.

3.4 Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

4 POLICY

4.1 The Company is required under data protection laws to ensure that Information Assets containing Personal Data are not retained in a form which enables the identification of individuals for any longer than is necessary for the purposes for which the Personal Data have been collected. We must be able to justify our retention of Personal Data to the authority responsible for enforcing data protection laws in the UK, the ICO.

4.2 In practice what this means is that the Company must not retain the Personal Data contained within Information Assets for any longer than is necessary:

(a) For the operational purpose that the Personal Data was collected for, and which the relevant Data Subject has been informed of (i.e. in relevant privacy notices);

(b) In order to comply with any applicable statutory or regulatory retention requirements; or

(c) To enable the Company to exercise its legal rights and/or defend against legal claims.

4.3 Where a statutory or regulatory retention requirement applies, or where data is relevant to an actual or potential legal claim, only the specific Personal Data which is required to be retained in order to meet the statutory/regulatory retention requirement or for a legal claim, should be retained for those purposes.

4.4 Personal Data may also be retained for a longer period if it is solely for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes, in accordance with Article 89(1) of the GDPR, subject to the implementation of appropriate technical and organisational measures which are required by data protection laws, in order to safeguard the rights and freedoms of the Data Subject. If you believe that Personal Data should be retained for these purposes, please contact the Data Protection Manager.

4.5 We must take a proportionate approach to data retention, balancing our needs with the impact of retention on Data Subjects' privacy. We also need to comply with all other aspects of data protection laws in relation to the Personal Data we retain, including ensuring that its retention is fair and lawful and that it is secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

4.6 Guideline data retention periods for different types of Personal Data, which should be followed by all employees, are provided in the Data Retention Matrix. However, earlier deletion may be appropriate in some circumstances. For example, if the Company is not actually using a record and it does not need to retain it to comply with a statutory or regulatory retention requirement or to enable the Company to exercise its legal rights and/or defend against legal claims. If you believe this is the case, please contact the Data Protection Manager to reconsider whether the Company needs to retain such records.

4.7 We must ensure that any request received from a Data Subject asking us to delete or destroy their Personal Data under the 'right to be forgotten' is dealt with in accordance with data protection laws. Any such request should be dealt with in accordance with our Individual Rights Guidance, which can be viewed at http://www.habasit.com/assets/Individual_Rights_Policy_Habasit_UK.pdf.

4.8 Each Information Asset owner must ensure that effective processes are in place to ensure that the Personal Data within their control is retained, archived and deleted or destroyed in accordance with this policy and the Data Retention Matrix.

4.9 Prior to the expiry of the retention period for the Personal Data provided in the Data Retention Matrix (or at regular intervals, and at least annually if no such retention period is provided), the Personal Data should be reviewed by the Information Asset owner to determine whether the Company should continue to retain it (or any part of it), for operational reasons, in order to comply with a statutory retention period or a regulatory obligation or for the purposes of a legal claim. If the Information Asset owner believes that the Personal Data needs to be retained for longer than a data retention period provided in the Data Retention Matrix, they should contact the Data Protection Manager.

4.10 If Personal Data needs to be retained only for statutory or regulatory purposes or for a legal claim, the Information Asset owner should ensure that it is moved from a live environment to a secure archive that is subject to appropriate security and restricted access to ensure that the Personal Data is only used for that specified purpose. Once it is no longer needed for that purpose, it is the responsibility of the Information Asset owner to ensure that the Personal Data is securely and permanently deleted or destroyed or anonymised in accordance with paragraph 6 of this policy.

4.11 Any queries about the applicable retention period for Personal Data within an Information Asset (for example, if there is no applicable data retention period in the Data Retention Matrix for that data) should be directed to the Data Protection Manager.

5 SECURE DELETION/DESTRUCTION OR ANONYMISING DATA

5.1 Where there is no need to retain Personal Data any longer, it is the responsibility of the Information Asset owner to ensure that the Personal Data is securely and permanently deleted or destroyed in accordance with this policy or that it is anonymised. Personal Data is anonymised where no Data Subjects can be identified from the data, either from that data alone or together with other data that the Company holds, has access to or may obtain access to. This also applies to any back-ups or duplicate copies of the Personal Data.

5.2 Personal Data must be deleted or destroyed using one of the following secure methods:

(a) Documents retained electronically should be deleted with a secure deletion utility that ensures that the information cannot be retrieved. Standard deletion utilities that only remove the file pointer should not be used.

(b) Personal Data on hard drives, removable media and any similar items must be securely erased before any disposal or reassignment of the equipment. Accepted methods include utilities that meet the DoD 5220 22-M standard or by encrypting the entire contents of the medium to at least AES-256 and irretrievably deleting the encryption key.

(c) Where Personal Data cannot be erased from equipment, it must be physically destroyed by an authorised, specialist destruction company, and certificates of destruction must be obtained.

(d) Paper copies must be destroyed using cross-cut shredders.

5.3 The Information Asset owner must approve the destruction or deletion of the Personal Data in advance and must record it including the date (and time if relevant), the content of the Personal Data and the method of destruction or deletion. They must also liaise with the Data Protection Manager to ensure that our Records of Processing Activities are amended accordingly.

6 CHANGES TO THIS POLICY

6.1 We reserve the right to change this policy at any time without notice to you so please check back regularly to obtain the latest copy of this policy. We last revised this policy in December 2018.

Schedule 1

Data Retention Matrix

Guideline Retention Periods

The retention periods below are guidelines only based on the type of record. It may be necessary to retain a specific record for longer than the guideline retention period or to delete it earlier, depending on the circumstances, such as its relevance to a particular type of legal claim.

This Data Retention Matrix should be read in conjunction with Habasit's Data Retention Policy, which explains how this matrix should be used in order to assist Habasit to comply with its data retention obligations under data protection laws.

Employee Records

Type of record	**Retention period**
Recruitment records These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. Criminal records checks.	For unsuccessful candidates 6 - 12 months after notifying candidates of the outcome of the recruitment exercise. These records may be transferred to a successful candidate's personnel file if they are relevant to the ongoing employment relationship.
Immigration checks	Three years after the termination of employment.
Contracts	
These may include: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Collective agreements	
Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for seven years after employment ends.
Payroll and wage records	
Payroll and wage records. Details of overtime. Bonuses. Expenses. Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they should be retained for seven years after employment ends.

Current bank details	3 years after the end of the tax year in which the last payment was made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they should be retained for seven years after employment ends.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they should be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they should be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel records	
These include: Qualifications/references. Consents for the processing of special categories of personal data. Annual leave records. Annual assessment reports. Disciplinary procedures. Grievance procedures. Death benefit nomination and revocation forms. Resignation, termination and retirement.	While employment continues and for seven years after employment ends.
Records in connection with working time	
Working time opt-out	Three years from the date on which they were entered into. However, if they may be relevant to disputes they should be retained for the duration of the relevant limitation period.
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.

Maternity records	
These include: Maternity payments. Dates of maternity leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends. However, if they may be relevant to a dispute they should be retained for the duration of the relevant limitation period.
Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made. However, if they may be relevant to disputes they should be retained for the relevant limitation period.

Schedule 2

Definitions

Controller	A controller determines the purposes and the means of the processing of personal data. It has the power to make high-level decisions about how and why the personal data can be used. It determines matters such as, the content of the data to be collected and used, who it will be collected about and when it will be disclosed and to whom.
Data Subjects	The individuals to whom the Personal Data relates, such as employees or job applicants, customers or suppliers.
European Economic Area (EEA)	The member countries of the European Union plus Norway, Iceland and Lichtenstein.
European Union	The member countries of the European Union are listed on this link: https://europa.eu/european-union/about-eu/countries_en
ICO	Information Commissioner's Office – the data protection regulator in the UK.
Information Asset	A piece or body of information (regardless of the form it takes, i.e. paper, electronic records or correspondence, photographs, CD/DVDs, CCTV etc.) such as an employee record, a customer list, or a financial report that is processed by or on behalf of the Company.
GDPR	The General Data Protection Regulation (EU) 2016/679
Personal Data	Any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified either directly from data, or indirectly, either on its own or together with other data which is in, or may come into, the Controller or Processor's possession. For example by reference to a name, identification number, location data, IP address, online identifier or to other factors such as physical or economic factors. This term will include any data that can be used to learn, record or decide something about an individual.
Personal Data Breach	A 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 or Processing	Any operation or set of operations carried out in relation to personal data, such as collecting, storing, disclosing, amending and deleting. Processing is widely defined and will in effect cover any activity involving personal data, for example, storing CVs, updating employee, customer or supplier records, monitoring employees' internet use or operating a CCTV system which captures Data Subjects' behaviour, etc.
Processor	A processor merely processes the personal data on behalf of the Controller. It is not able to make high-level decisions about how and why the data will be used.
Records of Processing Activities	The records of processing activities required to be created and maintained by the Company under Article 30 of the GDPR.
Special Categories of Personal Data	Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life/sexual orientation, genetic data or biometric data for the purpose of uniquely identifying a natural person.
Supervisory Authority	The regulatory authority responsible for enforcing data protection laws in a particular Member State.