

# Group Standard Operating Document

## Henry Bath Group Privacy Notice

<b>Document Details</b>
<b>Reference</b> HB_RC_PN
<b>Version</b> 1
<b>Approval date</b> December 2024
<b>Applicability</b> All Data Subject and Stakeholders with whom Henry Bath Group conducts business.
<b>GSOP Owner</b> Henry Bath Group Head of Risk

## Contents

	Contents.....	1
1	Introduction .....	2
1.1	Scope .....	2
2	Definitions .....	3
2.1	Data Controller .....	3
2.2	Data Processors .....	3
2.3	Data Authority .....	3
2.4	Personal Data .....	3
2.5	Sensitive Personal Data .....	4
2.6	Cookies .....	4
3	Roles & Responsibilities.....	4
4	Related policies and procedures.....	5
5	Personal data storage.....	5
5.1	Paper records.....	5
5.2	Electronic records.....	5
6	Personal data processing .....	6
6.1	Personal data accuracy.....	6
6.2	Disclosing personal data.....	6
7	Rights and choices .....	7
7.1	Subject Access Requests .....	7
7.2	Right to Erasure .....	7
8	Data protection – design and default.....	7
9	Data retention .....	8
10	Data destruction / disposal .....	8
11	Raising a concern.....	8
12	APPENDIX 1 – Data Retention Schedule.....	9

# 1 Introduction

---

This purpose of this document is to set out how Henry Bath Group process personal data in accordance with data protection laws.

This document provides guidance regarding the handling, storage and disposal of personal data, and the retention periods for key documents.

Henry Bath Group needs to gather and process certain information regarding individuals to conduct its business efficiently and compliantly. This may include information on customers, suppliers, business contacts, employees, and other individuals whom the organisation has a relationship with or may need to contact.

This statement describes how this personal data is collected, handled, stored, and deleted to meet our data protection standards and to comply with law.

This policy ensures that Henry Bath Group:

- Complies with applicable data protection law and follows best practice.
- Protects the rights of data subjects.
- Is transparent and open about how it stores and processes data; and
- Protects itself from the potential risks of a data breach.

This document also defines the Henry Bath Group Data Retention Policy to ensure compliance with legal, regulatory, operational and requirements.

## 1.1 Scope

The Henry Bath Group Privacy Notice is based on the principles of the UK Data Protection Act 2018. And the UK GDPR.

Henry Bath Group endeavours to comply with data protection laws and regulations in all countries in which the group operates, with the minimum standard applied being that found within the UK Data Protection Act 2018 and the UK GDPR. The Regulation enhances privacy rights for individuals and provides a strict framework within which commercial organisations can legally operate.

The retention schedule detailed in the Henry Bath Group Data Protection Policy is based on legal and operational requirements for each Henry Bath subsidiary.

The Henry Bath Group Privacy Notice covers all applicable personal data processed by Henry Bath Group. Categories of individuals include, but are not limited to, employees (current, previous and potential), agency workers, temporary labour, employee next of kin, clients, suppliers and visitors to Henry Bath Group sites (including contractors and drivers).

Personal data processed or stored electronically or as part of a paper filing system is covered under this statement. Electronic records include documents, systems and email correspondence containing personal data of Data Subjects.

## 2 Definitions

---

### 2.1 Data Controller

As the Group Parent Company, Henry Bath & Son Limited is the registered Data Controller for all Henry Bath Group subsidiaries. For the purposes of data protection laws and processing activities, Henry Bath & Son Limited is registered with the Information Commissioners Office (ICO) in the UK as Data Controller on behalf of the Henry Bath Group subsidiaries.

### 2.2 Data Processors

Henry Bath Group subsidiaries are considered data processors. Group subsidiaries are listed as follows:

- Henry Bath BV (Registered in the Netherlands)
- Henry Bath BVBA (Registered in Belgium)
- Henry Bath LLC (Registered in Michigan, USA)
- Henry Bath Singapore Pte Ltd (Registered in Singapore)
  - Henry Bath Singapore Pte Ltd Korean Branch (Registered in the Republic of Korea)
  - Henry Bath Singapore Pte Ltd Malaysia Branch (Registered in Malaysia)
- Henry Bath Warehousing (Shanghai) Co Ltd (Registered in China)

### 2.3 Data Authority

As the Group Parent Company, Henry Bath & Son Ltd is the registered Data Controller with the Information Commissioners Office; with 10 Princes Parade Liverpool, UK being the primary location for any data processing activities, cross-border processing controls and central registration as the Data Controller for Henry Bath Group business.

Henry Bath and Son Limited's registration details are available for public view on the ICO website: [Henry Bath and Son Limited ICO Registration](#)

### 2.4 Personal Data

For the purposes of Henry Bath Group data processing, Personal data is defined in line with UK Data Protection Act 2018 and the UK GDPR.

Personal Data means any form of data which relates to a living individual that can be identified from it directly or indirectly. Also referred to as Personally Identifiable Information (PII), or Personal Information (PI), personal data includes data recorded on computers, databases or on paper, expressions of opinion about the individual and indications of intentions towards them. This individual is known as the 'Data Subject'.

Examples of personal data are as follows:

- Name
- Date of birth
- Contact details such as address, telephone number and email address, including professional contact details.
- Identity numbers (including national insurance, social security, and citizen service numbers)
- Salary, benefits, and tax information
- Work performance records
- Work attendance records
- Education history

- Work history
- Credit ratings and history
- Banking information
- Photographs and recorded images
- Online identifiers (e.g., cookies, IP addresses)

## 2.5 Sensitive Personal Data

Sensitive personal data is that which the loss, theft, or misuse of could cause significant risk to a Data Subjects fundamental rights and freedoms, for example, data which could put them at risk of unlawful discrimination.

Examples of sensitive personal data are as follows:

- Religious beliefs
- Race and ethnic origin
- Trade union membership
- Health information
- Political opinions
- Criminal record history
- Sexuality

Henry Bath Group will not collect or process any sensitive personal data.

## 2.6 Cookies

When visiting our website or portal, a technology called "cookies" may be used to provide you with tailored information. A "cookie" is a tiny element of data that a web site can send to your browser, which may then be stored on your hard drive so we can recognize you when you return. You may be able to set your browser to notify you when you receive a cookie. Our cookies collect the operating system and browser that a visitor is using.

## 3 Roles & Responsibilities

---

### Henry Bath Group Compliance Team:

- Responsible for identifying and monitoring the storage, use and transfers of data, and ensure this is in line with this policy.
- Responsible for the Henry Bath Personal Data Register.
- Responsible for maintaining the Henry Bath Group Privacy Notice and Henry Bath Group Data Protection Policy
- Responsible for providing training and information regarding employees' data protection obligations.
- Responsible for monitoring overall compliance with this policy and being a point of contact for data protection related enquiries.

### Henry Bath Group Head of Risk:

- Responsible for reviewing written transfer agreements with authorised external recipients.
- Responsible for ensuring that this policy is implemented and operated in a reasonable and fair manner.
- Responsible for providing advice and guidance to individual members of staff and line managers.

**Henry Bath Group Management:**

- Responsible for ensuring processes employed across the business support the implementation of this policy.

**Henry Bath Group Employees, stakeholders and associated third parties:**

- Responsible for complying with this document.
- This policy is applicable to all group employees and associates of all Group subsidiaries without exception.

## 4 Related policies and procedures

---

Any Henry Bath Group policy that involves the handling of personal data should be read in consultation with the Henry Bath Group Privacy Notice, but the following policies are of particular note:

- Henry Bath Group Privacy Notice
- Henry Bath Group Data Protection Policy
- Policy 3 – Equality, diversity, and inclusion
- Policy 4 – Company ethics

## 5 Personal data storage

---

### 5.1 Paper records

Henry Bath Group store personal data electronically (in accordance with section 5.2) wherever possible.

When personal data must be stored on paper, it will be kept in a secure place (such as locked filing cabinet) with access permitted only to authorised individuals. This also applies to personal data which has been printed from an electronic format.

Data printouts are disposed of securely via confidential waste bins when no longer required.

### 5.2 Electronic records

When personal data is stored electronically, it is protected from unauthorised access, accidental deletion or manipulation, and any potential malicious hacking attempts.

The following key controls apply:

- Personal data is protected by strong passwords that are changed regularly and never shared between employees (unless for a shared document on a strict 'need-to-know' basis).
- In general, Henry Bath do not permit the use of removable media devices. On the occasions where these are permitted (e.g., USB flash drive, DVD), any devices must be kept locked away securely when not in use.
- Data is only stored on designated drives and servers, and is only uploaded to cloud computing services that have been approved by the Henry Bath Group Head of IT.
- Servers containing personal data are sited in a secure location, away from general office space, with access permitted to designated individuals only. All servers and computers containing personal data are protected by approved security software and a firewall.
- Data is backed up frequently. Those backups are tested regularly, in line with the Henry Bath Group standard backup procedure.
- Data is not saved directly to laptops or other mobile devices like tablets or smartphones.

## 6 Personal data processing

---

Henry Bath Group process Personal Data to provide our services, maintain our records, and meet our legal obligations. In addition, data from you, or generated during the course of our relationship with you, is also used for the purpose of reporting, monitoring and evaluation of services, as permitted by applicable law.

Henry Bath Group will not process any Personal Data for any other purpose than defined by this Privacy Notice and, in line with the conditions defined UK Data Protection Act 2018 and UK GDPR, we shall ensure the conditions for processing fall into one of more of the following categories:

- Contract Performance.
- Legal Obligation.
- Vital Interest.
- Public Interest; and more specifically,
- Legitimate Interest.

When personal data is accessed and used, there is a risk of it being subject to loss, corruption, or theft. The below is followed to maintain the security of data in use: .

- Personal data is only transferred to authorised internal and external recipients as detailed in the Henry Bath Group Personal Data Register.
- Transfers to external recipients are supported by a written agreement which has been reviewed by the Henry Bath Group Head of Risk.
- Personal data is not shared informally internally nor with those outside the organisation.
- Personal data is encrypted and/or protected before being transferred electronically. Further information on encryption and protection for data transfers can be provided by the Group Head of IT.
- Personal data concerning EU/EEA citizens is not transferred outside of the European Economic Area unless authorised to do so by the data subject. This includes to other Henry Bath Group subsidiaries.
- Employees do not save copies of personal data to their own computers. Personal data is always accessed and processed via the approved Henry Bath Group drives within restricted access folders.

### 6.1 Personal data accuracy

It is the responsibility of all employees who work with personal data to take reasonable steps to ensure the information is kept as accurate and as up to date as possible. Personal data storage is limited to as few places as necessary. Henry Bath Group will make it easy for individuals to correct any inaccurate information we hold about them. If any inaccuracies are discovered please contact [DataProtection@HenryBath.com](mailto:DataProtection@HenryBath.com)

### 6.2 Disclosing personal data

In certain circumstances, Henry Bath Group may be required to disclose personal data to law enforcement agencies without the consent or knowledge of the Data Subject.

Under those circumstances, the disclosure will be handled by the Henry Bath Group Head of Risk. All steps will be taken to ensure that the request is legitimate and approval will be sought from legal advisors where necessary.

## 7 Rights and choices

---

Henry Bath Group respect the information that is shared with us and understand it is the Data Subjects right to know how this data is processed and how to exercise rights to ask us to stop processing it.

Under the UK Data Protection Act 2018 and UK GDPR, and subject to certain conditions, individuals have the following rights relating to Personal Data:

- The Right to Rectification.
- The Right to Access.
- The Right to Erasure.
- The Right to Restrict Processing.
- The Right to Object; and
- The Right to Data Portability.

Data Subjects can exercise their rights associated with data processing at any time by contacting the Henry Bath Group Data Protection Officer by emailing [DataProtection@HenryBath.com](mailto:DataProtection@HenryBath.com)

### 7.1 Subject Access Requests

Data Subjects can request details about the personal data processed by Henry Bath Group by submitting a Subject Access Request to the Henry Bath Group Head of Risk by emailing [DataProtection@HenryBath.com](mailto:DataProtection@HenryBath.com) . Alternatively, requests can be made verbally to your Henry Bath Group contact or via post to:

FAO: Group Head of Risk  
Henry Bath Group  
10 Princes Parade,  
Liverpool  
L3 1BG  
United Kingdom

Once the request is received and relevant identities are verified, Henry Bath Group will work to provide you with the requested information, or provide access to your personal data within the defined timescales.

### 7.2 Right to Erasure

Subject to certain conditions, Data Subjects can request deletion of their personal data from Henry Bath Group internal systems. To make this request please contact the Henry Bath Group Head of Risk by emailing [DataProtection@HenryBath.com](mailto:DataProtection@HenryBath.com) .

Where possible, the Henry Bath Group Data Protection Officer will make provisions to process your request internally and will respond with a decision and /or confirmation once completed.

## 8 Data protection – design and default

---

Henry Bath Group has a responsibility to protect any personal data it collects. This means that data protection is embedded into all activities concerning personal data. This is referred to as **Data Protection By Design And Default**.

Data protection is considered in the initial design stage of all systems, services, and processes, and then throughout the lifecycle, and the protection of the rights and freedoms of individuals as default. This includes, but is not limited to:

- The development of IT systems which process personal data.
- Organisational processes which have privacy implications.
- Physical design of Henry Bath Group premises to ensure security of personal data.
- Sharing data with third parties and processors.

- Collecting personal data for new purposes or the collection of new data sets.

## 9 Data retention

---

Henry Bath Group do not keep data, whether personal or non-personal, for longer than it is necessary to fulfil its intended purpose. Retention periods for specific categories of data are detailed in the Data Retention Schedule (Appendix 1).

## 10 Data destruction / disposal

---

Once the personal data has reached its maximum retention period, Henry Bath Group ensures it is destroyed securely.

- Paper copies are shredded or disposed of via confidential waste bins, which are collected periodically by an approved contractor.
- Electronic copies are deleted.

## 11 Raising a concern

---

If you have knowledge, or suspicion, that any person data which is being processed by, or on behalf of, Henry Bath Group has been, or is at risk of being, subject to a data breach please contact the Henry Bath Group Data Protection Officer immediately by emailing [DataProtection@HenryBath.com](mailto:DataProtection@HenryBath.com).



## 12 APPENDIX 1 – Data Retention Schedule

The Data Retention Schedule applies to all key records across the Henry Bath Group, including those that contain personal data. The following key retention periods apply:

Category of Records	Record	Retention Period	Exceptions
Financial	Accounting transactions and accounts	6 years	
	Fixed assets	6 years	
	Frauds and investigations	6 years	
	Purchasing and requisition	6 years	
	Statutory accounts / reports	6 years	
	Tax records	6 years	
	External audit reports	6 years	
Commercial	Contracts, leases etc.	6 years	
	Client details for events	6 years	
	Correspondence with clients	6 years	
Human Resources and Employee data	Recruitment records for unsuccessful candidates	1 year from date of end of engagement	
	Recruitment records for successful candidates	6 years from termination of employment	
	Screening results	6 years from termination of employment	
	Payroll and benefits records	6 years from termination of employment	
	Bank details for payroll and expenses	6 years from termination of employment	
	Performance reviews	6 years from termination of employment	
	Disciplinary records	6 years from termination of employment	
	Grievance records	6 years from termination of employment	
	Absence and attendance records	6 years from termination of employment	
	Pension records	6 years from termination of employment	
	Details for travel bookings	6 years from termination of employment	
	Leaver emails and H: drives	6 years from termination of employment	

	Proof of Right to Work	6 years from termination of employment	
	Personnel files	6 years from termination of employment	
	Leaver records	6 years from termination of employment	
	Job files	6 years	
	CCTV recordings	Maximum 90 days after data recorded	
	Maintenance records	6 years	
	Health & Safety incident reports	10 years	
	Visitor / contractor records	6 years	
	Customs records	6 years	
	Exchange compliance records	6 years	
Legal	Workers' compensation claims	6 years from termination of employment	
	Litigation and claims	6 years from termination of employment	
IT	HB One Drive	3 Years restore	
	Emails	2 Years (with possible exceptions)	
	WMS	Currently indefinite	
	Client Portal	Currently indefinite	
	User One Drive	2 Years	