≈≈≈≈≈≈≈≈≈

1	Introduction	1

1.1. This Personal Data Retention and Destruction Policy (this "policy") sets out the obligations of Polyco Healthline Limited ("Polyco Healthline", "we", "us", "our") regarding retention of the Personal Data we collect, hold and process. The purpose of this policy is to set out the basis and periods for which we will retain Personal Data and how, where possible we will dispose of Personal Data. This will ensure compliance with our legal obligations and effective data management.

1.2. This policy applies to all employees, workers, contractors, consultants and interns ("personnel", "you", "your"). Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action, up to and including termination of your contract for serious offences.

1.3. This policy has been prepared with due regard to the data protection laws applicable to us and our Personal Data processing activities. These data protection laws include the UK General Data Protection Regulation ("UK GDPR") and/or the EU General Data Protection Regulation 2016/679 ("EU GDPR") (whichever is applicable) and the Data Protection Act 2018 ("DPA18"), (collectively referred to as the "Data Protection Law").

1.4. This policy should be read together with the following related documents:

a) Polyco Healthline Data Protection Policy

Please note, that the definitions for any undefined terms in this policy can be found in our Data Protection Policy and are applicable to this policy.

2.1 We place high importance on respecting the privacy and protecting the Personal Data of individuals whose Personal Data we collect and process as a Data Controller. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals where we are a Data Controller. Our policy is to comply, not only with the letter of the law, but also with the spirit of the law.

3.1 This policy applies to all Personal Data processed by us, or on behalf of us (such as Personal Data in hosted or cloud systems) and whether held in electronic or physical records. This includes Personal Data in structured records (such as databases), unstructured records (such as documents and spreadsheets), in emails, in audio and video recordings and includes Personal Data we generate (such as through access control systems and in personnel files) as well as Personal Data provided to us.

4.1 We will ensure that the records we process containing Personal Data are properly and carefully managed in accordance with this policy and the applicable Data Protection Law.

4.2 We will keep track of our records, ensuring that they are:

- processed fairly, lawfully, and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date; and
- processed securely.

4.3 Only the information required for the purpose will be collected and we will be open and transparent with individuals in relation to what we do with their information. Access to records will be limited to what is required for the given situation and we will make regular checks to ensure the records are accurate and, where necessary, kept up to date. We shall also ensure that the records are kept securely in accordance with our Information Security Policy and our obligations under the Data Protection Law to implement appropriate technical and organisational measures to safeguard Personal Data are met.

4.4 Our robust records management will ensure that our records are:

- clearly and appropriately classified, labelled and indexed;
- subject to appropriate access controls;
- stored securely;
- in a usable format;
- securely and permanently disposed of in accordance with the retention periods set out in the Retention Schedule annexed to this policy; and
- securely stored with rigid access controls (“put out of use”) where system limitations disallow us from disposing of personal data.

4.5 Adopting the above practice will enable us to:

- operate our company efficiently and with a consistent approach;
- locate and retrieve records in a timely manner, when required;
- protect and support individuals' rights;
- respond to enquiries from the supervisory authority promptly; and
- comply with the Data Protection Law.

4.6 In support of the above, we will maintain and regularly update our Record of Processing Activities ("RoPA"). This will identify the Personal Data processed by us and include:

- the type of Personal Data/Data File (e.g., complaint files);
- whether the records contain Personal Data, special category data or criminal offence data;
- the format of the records (hard copies, excel spreadsheets, PDFs etc);
- where they are held;
- who has access to them;
- who they are shared with;
- how long they are retained; and
- how they are kept secure.

5	Responsibilities	3

5.1 Key data protection responsibilities within Polyco Healthline are as follows:

- the Board of Directors is accountable for ensuring we meet our data protection obligations;
- the GDPR committee (IT Manager, Head of HR, IT Manager) is responsible for implementing and enforcing this policy;
- Line managers are responsible for ensuring that personnel under their management are made aware of, and adhere to, this policy;
- all personnel working with Personal Data are responsible for ensuring it is kept securely, is accessible only to those who need to use it and is not disclosed to any third party other than as required or where authorised by the GDPR committee; and
- all personnel are required to read, understand and adhere to this policy when processing Personal Data on our behalf.

6	Data Retention Principles	4

6.1 The following data retention and disposal principles shall apply to all processing:

- Personal Data shall not be retained for longer than is necessary for the purposes for which the Personal Data are processed (where technically possible); and
- Once Personal Data has reached the end of its life, (where technically possible) the data or the record holding the data shall be securely and permanently disposed of in a manner that ensures it can no longer be used. Where disposal is not technically possible, the personal data will be stored securely with rigid (limited) access controls implemented ("put out of use").

6.2 Meeting these principles helps ensure we manage risks to rights and freedoms of Data Subjects associated with processing their Personal Data, facilitate Data Subject rights, meet our legal obligations and improve the quality and efficiency of our data management.

6.3 Where we are the Data Controller, these principles shall govern the retention and destruction of Personal Data.

7	Data Retention Periods	4

7.1 Polyco Healthline as a Data Controller

7.1.1 Personal data shall be retained for no less than the minimum retention periods and no longer than the maximum retention periods set out in the retention schedule at Schedule 1 (the "Retention Schedule").

7.1.2 In certain situations, Personal Data may be kept for longer than as set out in the Retention Schedule, but only where the GDPR Committee has given their approval in writing and where we have reasonable grounds for retaining the Personal Data beyond the retention period. Examples include situations where:

a) the Personal Data is required for the exercise or defense of legal claims, and appropriate technical and organisational measures have been applied to the continued retention of the Personal Data to protect the risks to rights and freedoms of Data Subjects;
b) the Personal Data is required by us for statistical purposes and appropriate safeguards (pursuant to Article 89(1) of the UK/EU GDPR have been applied to the processing for these purposes to protect the risks to rights and freedoms of Data Subjects;
c) the Personal Data has been fully and effectively anonymised and the GDPR Committee is satisfied that Data Subjects cannot be identified from the anonymised data.
d) it is not technically possible to dispose of the personal data (limited by systems functionality).

7.1.3 When establishing or reviewing Personal Data retention periods, the following shall be taken into account:

a) the purpose(s) for which the Personal Data is collected and processed;
b) the lawful basis upon which the Personal Data is collected and processed;
c) whether the Personal Data is special category Personal Data or relates to criminal convictions or offences;
d) the risks to rights and freedoms of Data Subjects associated with collecting, holding and processing the Personal Data;
e) our legal or regulatory obligations to collect or retain the Personal Data in question; and
f) our objectives and requirements when collecting and processing the Personal Data

8	Data Disposal	5-6

8.1 Polyco Healthline as a Controller

8.1.1 Personal data shall be disposed of in the following circumstances:

a) on expiry of the retention period set out in the Retention Schedule (where technically possible);

b) in response to a request from a Data Subject to erase their Personal Data where our Subject Rights Request Procedure has been followed and the GDPR Committee has confirmed the Personal Data should be destroyed;

c) at the discretion of the GDPR Committee, where retention of the Personal Data is no longer necessary for the purpose of the processing prior to the expiry of the relevant retention period and the GDPR Committee has confirmed the Personal Data should be destroyed.

8.1.2 Where Personal Data is erased at the request of a Data Subject, we may retain such limited Personal Data as is reasonably necessary to keep a record of the erasure for the purposes of demonstrating compliance and enforcing erasure across all business systems, provided appropriate technical and organisational measures have been applied to the retained data in order to protect the risks to rights and freedoms of the Data Subject.

8.1.3 Personal data is to be erased, destroyed or otherwise disposed of as follows:

a) Personal Data held in electronic records (including back-ups) is to be securely deleted using appropriate tools approved by the GDPR Committee (where technically possible).

b) Sensitive Personal Data held in electronic records (including back-ups) is to be securely deleted using appropriate tools approved by the GDPR Committee (where technically possible).

c) Hard copy Personal Data held in physical records (including archives) is to be cross-cut shredded and disposed of as 'confidential waste' using locked rubbish bins for collection by a disposal supplier approved by the GDPR Committee.

d) Special Category or other Sensitive Personal Data held in physical records (including archives) is to be disposed of as 'confidential waste' to consist of cross-cut shredding and incineration by a disposal supplier approved by the GDPR Committee.

8.1.4 In all cases, proof of destruction is to be recorded. Where an external disposal supplier is used, a certificate of destruction must be provided by the supplier and an appropriate data processing agreement should be entered into.

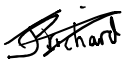
8.1.5 Electronic or physical records may contain different types of Personal Data which are used for different purposes. These different types of Personal Data may be subject to different retention periods or have different levels of sensitivity. It is therefore imperative that the data are managed, not just the records. It may be necessary to destroy some Personal Data from a record, but not other Personal Data or information from within the same record.

8.1.6 We endeavor to ensure that our records management system is designed in a way that allows for different retention periods to be applied to different types of Personal Data within the same record, in accordance with the data protection by design and default requirements under the Data Protection Law. However, if, due to technical reasons, it is not possible to permanently and securely destroy electronic Personal Data which is scheduled for destruction, it will be put 'beyond use'. This means that it will not be treated as 'live' data, as it will not be used, accessed or shared, but will be kept securely, using appropriate technical and organisational measures. The guidance from the UK Supervisory Authority, the Information Commissioner's Office, is that following these procedures will have the effect of suspending data protection compliance issues. However, we will strive to ensure that no such deletion and retention issues arise.

9	Implementation and Policy Management	6

9.1 This policy shall be deemed effective as of 01.02.2022. No part of this policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

9.2 This policy will be reviewed by the GDPR Committee annually and following any Personal Data breach.

Signature: 

Name: Jack Prichard

Position: Chief Executive Officer

Place of Issue: Bourne, PE10 0DN, UK

Date: 11th June 2024

Schedule 1

Retention Schedule

Category of Personal Data	Contains Personal Data	Retention Period	Rationale for Retention Period
Polyco Healthline contact details	Yes	*Trigger:* each purchase order *Maximum:* 7 years	Contractual limitation. If a prospective customer does not place an order within a year of their enquiry, all of their Personal Data shall be deleted after one year, where technically possible. If consent was the lawful basis for processing the data, that consent may be withdrawn at any time.
Supplier contact details	Yes	*Trigger:* each purchase order *Maximum:* 7 years	Contractual limitation. If Polyco Healthline does not place an order within a year of their enquiry, where technically possible, all of their Personal Data shall be deleted after one year. If consent was the lawful basis for processing the data, that consent may be withdrawn at any time.
Customer financial transaction details	Yes	*Trigger:* upon voluntary termination of Agreement or receipt of purchase order *Maximum:* 7 years	In accordance with the Companies Act 2006 – 6 years from the end of the last company financial year they relate to, where technically possible. If not technically possible this data will be "put out of use".
Customer account transactions	Yes	*Trigger: each account interaction.* *Maximum:* 7 years	Contractual limitation. If not technically possible this data will be "put out of use".
CCTV Recordings	Yes	*Trigger:* record created *Maximum:* 30 days	*This data is kept for up to 30 days after which the surveillance system will automatically overwrite previous data.*
HR files other than as specified below	Yes	*Trigger:* termination of employment *Maximum:* 8 years	7 years. A claim in relation to a person's employment could be a breach of contract claim, which may be brought within 7 years.

Category of Personal Data	Contains Personal Data	Retention Period	Rationale for Retention Period
Payroll and wage records (including summaries of expenses, payments made on the employee's behalf)	Yes	*Trigger:* end of accounting period *Maximum:* 8 years	Compliance with tax legislation.
Job applications and interview records of unsuccessful candidates This includes unsolicited job applications and CVs	Yes	*Trigger:* notification the candidate was unsuccessful *Maximum:* 1 year	An Employment Tribunal case must be brought within 3 months. The longer retention period accounts for the fact that a tribunal has quite a wide discretion to extend the time period when it is "just and equitable to do so".
Accident reports and records, accident record books, health and safety policy, assessments	Yes	*Trigger:* record created *Maximum:* 45 years	Records which deal with assessments of health and safety risks and steps taken to reduce or prevent them should be kept until the regulations they obey are superseded or no longer relevant. However, it is advisable to keep all records relating to health and safety standards for at least 40 years in line with the Control of Substances Hazardous to Health Regulations (COSHH).
Employees' Pension Scheme Documentation	Yes	*Trigger:* Date employee is enrolled on to scheme *Maximum:* N/A	As there are no time limits in relation to when certain actions may be brought by beneficiaries, we hold pension related data indefinitely.
Immigration / right to work checks	Yes	Trigger: termination of employment / contract Maximum: 3 years	Compliance with the Immigration, Asylum and Nationality Act 2006.
Statutory Maternity Pay Records, calculations, certificates (Mat B1s) or other medical evidence	Yes	Trigger: Last day of Statutory Maternity leave Maximum: 4 years	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Subject Access Requests (SAR) - including information compiled for the purposes of meeting the request	Yes	Trigger: Date of last action related to the SAR Maximum: 2 years	To permit requestors to make any necessary appeals.