

Section	Title	Page
1	Introduction	1-2
2	Policy Statement	2
3	Scope	2
4	Definitions	2-3
5	Responsibilities	4
6	Data Protection Principles	4
7	Data Protection by Design and by Default	5
8	Data Processing Obligations	5-6
9	Accountability	6-7
10	Risk Management	7
11	Data Subject Rights	8
12	Protection of Personal Data	8-9
13	Data Retention and Destruction	9
14	International Data Transfers	9-10
15	Data Breach Notifications	10
16	Implementation and Policy Management	10
17	Schedule 1	11
18	Schedule 2	12

1	Introduction	1
---	--------------	---

- 1.1. This Data Protection Policy (this “Policy”) sets out the obligations of Polyco Healthline Limited (“Polyco Healthline”, “we”, “us”, “our”) regarding data protection and the rights of individuals whose Personal Data we collect, use and process in the course of our business activities.
- 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 or our other data protection policies and procedures 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, the EU General Data Protection Regulation 2016/679 (where applicable) (together the “GDPR”) and the Data Protection Act 2018 (“DPA 2018”), collectively referred to in this Policy as the “Data Protection Law”.

- 1.4. This Policy should be read together with the following related documents:
- Polyco Healthline Data Protection by Design & by Default Policy
  - Polyco Healthline Personal Data Retention and Destruction Policy
  - Polyco Healthline Information Security Policy
  - Polyco Healthline Data Subject Rights Procedure
  - Polyco Healthline Personal Data Breach Procedure
  - Polyco Healthline DPIA Procedure
  - Polyco Healthline EU Transfer Impact Assessment Template (where applicable)
  - Polyco Healthline UK Transfer Risk Assessment Template (where applicable)
  - Polyco Healthline Data Protection Monitoring Framework Guidance

<b>2</b>	Policy Statement	2
----------	------------------	---

- 2.1 We place high importance on respecting the privacy and protecting the Personal Data of individuals with whom we work including our clients, end customers and employees. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals. Our policy is to comply not only with the letter of the law, but also with the spirit of the law.

<b>3</b>	Scope	2
----------	-------	---

- 3.1 This Policy applies to all Personal Data processed by us, whether held in electronic form or in physical records, and regardless of the media on which that data is stored. It applies to the Personal Data we process as a Data Controller.
- 3.2 Polyco Healthline Limited is registered as a Data Controller with the Information Commissioner’s Office (“ICO”), registration number Z1836501.

<b>4</b>	Definitions	2-3
----------	-------------	-----

- 4.1 The following definitions apply across all our data protection policies, procedures and supporting documents:

Term	Description:
Accountability	A duty to answer to the success or failure of strategies, decisions, practices and processes.
Criminal Information	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings
Data Controller	A person, entity or organisation that determines the purposes and means of processing Personal Data.
DPA18	Data Protection Act 2018
Data Protection Officer	The Data Protection Officer is responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Law.

Term	Description:
Data Protection Law	UK General Data Protection Regulation, the EU General Data Protection Regulation 2016/679 (where applicable) (together the “GDPR” and the Data Protection Act 2018 (“DPA18”).
Data Processor	A person, entity or organisation that processes Personal Data on behalf of a Controller.
Data Subject	Any natural person (individual) whose Personal Data is being processed.
Data Protection Impact Assessment (“DPIA”)	A DPIA is designed to help an organisation assess the risks associated with data processing activities that could compromise the rights and freedoms of individuals. It can be used to identify and mitigate risk associated with a product, service, business process or other organisational change.
EU GDPR	EU Regulation 2016/679 General Data Protection Regulation
Legitimate Interest Assessment (“LIA”)	Determines if individual’s Personal Data is being used in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Personal Data	Any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
processing	Any operation or set of operations that is performed on Personal Data, such as collection, recording, organising, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, combination, restriction or erasure.
Information Commissioner’s Office (“ICO”)	An independent public body established in the UK responsible for monitoring the application of the UK GDPR, Data Protection Act 2018 and the Privacy & Electronic Communications Regulations.
Sensitive Personal Data	Special Category Data and Personal Data relating to criminal convictions and offences.
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, biometric data (where used to identify a data subject), data concerning health and data concerning a natural person’s sex life or sexual orientation.
UK GDPR	Has the meaning given to it in section 3(10) (as supplemented by section 205(4)) Data Protection Act 2018

5	Responsibilities	4
---	------------------	---

- 5.1 Key data protection responsibilities within Polyco Healthline are as follows:
- a) the Board of Directors is accountable for ensuring we meet our data protection obligations;
  - b) the GDPR Committee (Head of Digital, Head of HR, IT Security & Infrastructure Manager) is responsible for implementing and enforcing this Policy;
  - c) Line Managers are responsible for ensuring that personnel under their management are made aware of adhere and to this Policy;
  - d) all personnel working with Personal Data over which they have decision making authority 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 without the authorisation of a member of the Board; and
  - e) all personnel are required to read, understand, and adhere to this Policy when processing Personal Data on our behalf.
- 5.2 You should speak with the Head of Digital and Technology Solutions to ask a question, or raise a concern, relating to this Policy or to data protection in general.

6	Data Protection Principles	4
---	----------------------------	---

- 6.1 The following data protection principles shall govern the collection, use, retention, transfer, disclosure and destruction of Personal Data by us:
- **Principle 1 - Fair, Lawful & Transparent**  
Personal Data must be processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;
  - **Principle 2 - Purpose Limitation**  
Personal Data must only be collected and processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;
  - **Principle 3 - Data Minimisation**  
Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - **Principle 4 - Accuracy:**  
Personal Data must be accurate and kept up to date;
  - **Principle 5 - Storage Limitation:**  
Personal Data which permits identification of Data Subjects (i.e., data which has not been anonymised) must be kept for no longer than is necessary for the purposes for which the Personal Data are processed; and
  - **Principle 6 - Security:**  
Personal Data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental

loss, destruction or damage.

<b>7</b>	Data Protection by Design and by Default	5
----------	--	---

- 7.1 We shall ensure that the risks to rights and freedoms of Data Subjects associated with processing are key considerations when:
- a) Designing, implementing and during the life of business practices and processes that involve the processing of personal data (“processing activities”); and
  - b) Developing, designing, selecting, procuring and using applications, services, products and other IT systems and technologies for collecting, holding, sharing, accessing and otherwise processing personal data (“processing systems”).
- 7.2 This risk led approach to processing activities and processing systems shall apply throughout the full lifecycle of the processing, from initial planning and setting of specifications, during use of processing systems, through to disposal of the personal data. It shall consider both the likelihood and the severity of the potential harm to the rights and freedoms of Data Subjects.
- 7.3 Where the risk to rights and freedoms of Data Subjects is likely to be high, or where otherwise required by law or the relevant supervisory authority, a DPIA shall be performed in accordance with our DPIA procedure.
- 7.4 Safeguards and preventive measures shall be implemented into processing activities and processing systems from the outset and throughout the processing lifecycle, to mitigate the risks to data subjects and protect their rights. These safeguards and measures shall be proportionate to the risks and include organisational (e.g., policy, awareness, governance, and assurance) as well as technical measures (e.g., pseudonymisation). The objectives of such safeguards and measures shall include:
- a) data minimisation;
  - b) limiting the extent of the processing, storage, and access to what is strictly necessary;
  - c) ensuring transparency for data subjects regarding the processing activities; and
  - d) ensuring the security of the personal data.

<b>8</b>	Data Processing Obligations	5-6
----------	-----------------------------	-----

- 8.1 Polyco Healthline as a Data Controller
- 8.1.1 Where we are the Data Controller, Data Subjects must be provided with information notifying them of the purposes for which we will process their Personal Data (a “privacy notice”). When Personal Data is obtained directly, the privacy notice shall be provided to the Data Subject at the time of collection. When Personal Data is obtained indirectly, the privacy notice shall be provided to the Data Subject as soon as possible (and not more than one calendar month) after it is obtained from a third party. The privacy notice must

explain what processing will occur and must also include the information set out at Schedule 1 of this Policy.

- 8.1.2 Our use of the Personal Data must match the description given in the privacy notice and be limited to what is necessary for the specific purposes stated. Where our lawful basis for processing is based on our legitimate interests, we may only process the Personal Data if our legitimate interests are not outweighed by the interests, rights and freedoms of the Data Subjects in question. A legitimate interests assessment must be performed to confirm this.
- 8.1.3 We must not collect or process any more Personal Data than is strictly necessary for the purposes of the processing (“data minimisation”), as set out in our privacy notice, and must ensure that data minimisation continues to be applied throughout the lifetime of the processing activities.
- 8.1.4 Personal Data must be kept accurate and up to date. The accuracy of Personal Data must be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps are to be taken without delay to amend or erase that data, as appropriate. Personal Data must not be kept for any longer than is necessary for the purpose for which that data was originally collected and processed. When the data is no longer required, all reasonable steps must be taken to securely erase or dispose of it without delay, as set out at Section 12 of this Policy.
- 8.1.5 Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

<b>9</b>	Accountability	6-7
----------	----------------	-----

- 9.1 Only those personnel that need access to, and use of, Personal Data to carry out their assigned duties correctly will be permitted access to the Personal Data we hold. All personnel handling Personal Data on our behalf must be:
  - made fully aware of both their individual responsibilities and our responsibilities under this Policy and applicable law, and be provided with a copy of this Policy;
  - appropriately trained to do so and suitably supervised, with training to be provided upon commencing employment and refresher training to be provided at least annually; and
  - bound to handle the Personal Data in accordance with this Policy and the law by contract.
- 9.2 The methods of collecting, holding and processing Personal Data by personnel, or other parties working on our behalf, are to be regularly evaluated and reviewed by the GDPR Committee.
- 9.3 All consultants, agencies and other parties working on our behalf and handling Personal Data must ensure that all of their employees who are involved in the processing of Personal Data are held to the same obligations as Polyco Healthline personnel arising out of this Policy.

- 9.4 When using a Data Processor (or, where permitted, a Data sub-Processor), a binding contract must be implemented between us and the Data Processor, setting out the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the controller. Processor contracts must also include the terms set out at Schedule 2 of this Policy.
- 9.5 We will keep written internal records of processing activities in respect of all Personal Data collection, holding, and processing (“RoPA”).

9.6 Data Controller RoPA

Where we are the Data Controller, the RoPA will incorporate the following information:

- the name and contact details of the Data Controller, our Data Protection Officer or point of contact for data related concerns and any joint controllers;
- the purposes for which we process Personal Data;
- details of the categories of Personal Data collected, held, and processed by us; and the categories of Data Subject to which that Personal Data relates;
- details (and categories) of any third parties that will receive Personal Data from us;
- details of any transfers of Personal Data to countries outside the UK or European Economic Area (“EEA”) including all mechanisms and security safeguards;
- the envisaged retention periods for the different categories of Personal Data; and
- descriptions of the technical and organisational measures we have implemented to ensure the security of Personal Data.

<b>10</b>	Risk Management	7
-----------	-----------------	---

- 10.1 We will monitor the risks to Data Subjects associated with all existing and planned Personal Data processing activities and implement appropriate technical and organisational measures to safeguard Data Subjects and ensure the data protection principles set out in this Policy are met. This risk led approach to data protection will be applied across all our business activities to ensure data protection by design and by default, as set out in our Data Protection by Design and by Default Policy.
- 10.2 Where the risks to rights and freedoms of Data Subjects associated with any existing or planned Personal Data processing to be carried out by us are potentially high, or where otherwise required by applicable law or a supervisory authority in a country or territory in which we operate, we will carry out a Data Protection Impact Assessment (“DPIA”). All DPIAs are to be undertaken as set out in our Data Protection by Design and by Default Policy. A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of next review.

<b>11</b>	<b>Data Subject Rights</b>	<b>8</b>
-----------	----------------------------	----------

11.1 Data subjects have the following rights regarding Personal Data processing and the data that is collected and held about them:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (the 'right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights with respect to automated decision-making and profiling.

11.2 Where we are the Data Controller, we are responsible for facilitating Data Subjects' rights.

11.3 Requests by Data Subjects to exercise their rights must be facilitated as set out in our Data Subject Rights Procedure.

<b>12</b>	<b>Protection of Personal Data</b>	<b>8-9</b>
-----------	------------------------------------	------------

12.1 All personnel must comply with the following when working with Personal Data:

- Personal Data must be handled with care at all times and must not be shared with any colleague, who does not have access to it, or with any third party without authorisation;
- Physical records must not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time and must not be removed from the business premises without authorisation;
- If Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- All physical copies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked filing cabinet, drawer, box or similar;
- All electronic copies of Personal Data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised;
- Personal Data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication or equivalent service (such as a personal cloud service);
- Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this Policy and the Data Protection Law and all other applicable law (which may include demonstrating that all suitable technical and organisational measures have been taken and entering into a Data Processor contract with us);



- All Personal Data stored electronically shall be backed-up regularly and securely; and
- under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

12.2 In addition to the obligations set out above, all personnel involved in processing Personal Data are required to read and adhere to our Information Security Policy.

<b>13</b>	Data Retention and Destruction	9
-----------	--------------------------------	---

## Polyco Healthline as a Data Controller

13.1 Where we are the Data Controller, we may only retain Personal Data for as long as is reasonably required and in any event, only for as long as set out in our Personal Data Retention and Destruction Policy. Written authorisation from the Head of Digital and Technology Solutions is required to retain Personal Data for longer than as set out in the Personal Data Retention and Destruction Policy.

13.2 Once Personal Data records have reached the end of their life, they must be securely destroyed (where technically possible) or put out of use in a manner that ensures that they can no longer be used.

<b>14</b>	International Data Transfers	9-10
-----------	------------------------------	------

14.1 We will only transfer ('transfer' includes making available remotely) Personal Data from the UK to countries outside the UK where:

- the transfer is to a country (or an international organisation) that the UK Government and/or the European Commission has determined ensures an adequate level of protection ("Adequacy");
- Standard Contractual Clauses (SCCs) with supplementary measures adopted by the European Commission have been put in place between the entity in the European Economic Area ("EEA" – the 27 EU member states, plus Norway, Iceland and Liechtenstein) and the entity located outside the EEA;
- an International Data Transfer Agreement (IDTA) adopted by the UK government has been put in place between the entity in the UK and the entity located outside the UK;
- Binding Corporate Rules (BCRs) have been implemented, where applicable; or
- where the transfer is otherwise permitted by law.

14.2 Where a transfer is not based on Adequacy, we will undertake a Transfer Impact Assessment ("TIA") using our TIA Template for EU data transfers, or a Transfer Risk Assessment ("TRA") for UK data transfers, to ensure that Data Subjects (whose Personal Data is transferred) continue to have a level of protection essentially equivalent to that under the UK or EU GDPR (whichever is applicable). If the TIA/TRA outcome is that the appropriate safeguard does not provide the required level of protection, we will implement supplementary measures e.g., encryption.

<b>15</b>	Data Breach Notifications	10
-----------	---------------------------	----

15.1 All Personal Data breaches must be reported immediately to the GDPR Committee and must be added to the register of Personal Data breaches.

15.2 Polyco Healthline as a Data Controller

15.2.1 Where we are the Data Controller, if a Personal Data breach occurs which is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the relevant supervisory authority must be notified of the breach without delay, and in any event, within 72 hours of having become aware of it, if this is feasible. If the notification is not made within 72 hours, it should be made as soon as possible, together with reasons for the delay. The ICO is the supervisory authority in the UK


15.2.2 If a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects, all affected Data Subjects are to be informed of the breach directly and without undue delay.

15.2.3 All data breach notifications must be handled strictly in accordance with our Personal Data Breach Procedure and added to our Personal Data Breach Register which is located on the company intranet.

<b>16</b>	Implementation and Policy Management	11
-----------	--------------------------------------	----

16.1 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.

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

**Signature:** 

**Name:** Jack Prichard

**Position:** Deputy Chief Executive Officer

**Place of Issue:** Bourne, PE10 0DN, UK

**Date:** 17th March 2023

## Schedule 1

### Privacy Notices

Privacy notices for Data Subjects shall include:

- a) the identity and contact details of the Data Controller including, but not limited to, the identity of our Data Protection Officer and EU representative, where applicable;
- b) the purpose(s) for which the Personal Data is being collected and will be processed and the legal basis justifying that collection and processing;
- c) where applicable, the legitimate interests upon which we are justifying the collection and processing of the Personal Data;
- d) where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed;
- e) where the Personal Data is to be transferred to one or more third parties, details of those parties;
- f) where the Personal Data is to be transferred to a third party that is located outside of the UK/EEA (whichever is applicable), details of that transfer, including but not limited to, the safeguards in place;
- g) details of the length of time the Personal Data will be held (or, where there is no predetermined period, details of how that length of time will be determined);
- h) details of the Data Subject's rights;
- i) where applicable, details of the Data Subject's right to withdraw their consent to the processing of their Personal Data at any time;
- j) details of the Data Subject's right to complain to a supervisory authority;
- k) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it; and
- l) details of any automated decision-making that will take place using the Personal Data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

## Schedule 2

### Processor Contracts

Contracts with Data Processors who will process the Personal Data must set out the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the controller. They must also include terms requiring the Data Processor to:

- a) only act on the written instructions of the controller;
- b) ensure that people processing the data are subject to a duty of confidence;
- c) take appropriate measures to ensure the security of processing;
- d) only engage sub-Data Processors with the prior consent of the Data Controller and under a written contract;
- e) assist the Data Controller in providing subject access and allowing Data Subjects to exercise their rights under the GDPR;
- f) assist the Data Controller in meeting its GDPR obligations (or obligations under other applicable laws) in relation to the security of processing, the notification of Personal Data breaches and data protection impact assessments;
- g) delete or return all Personal Data to the Data Controller as requested at the end of the contract; and
- h) submit to audits and inspections, provide the Data Controller with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Data Controller immediately if it is asked to do something infringing the Data Protection Law (or other applicable legislation).