≈≈≈≈≈≈≈≈≈

1	Introduction	1

1.1. This Data Protection by Design & by Default Policy (this "Policy") sets out the obligations of Polyco Healthline Limited ("Polyco Healthline", "we", "us", "our") regarding data protection by design and by default in respect of the Personal Data we collect, hold and process in the course of our business activities.

1.2. This Policy applies to all our 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, 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:

a) Polyco Healthline Data Protection Policy
b) Polyco Healthline Personal Data Retention Policy
c) Polyco Healthline Information Security Policy
d) Polyco Healthline Data Subject Rights Procedure
e) Polyco Healthline Data Personal Data Breach Procedure
f) Polyco Healthline DPIA Procedure

2	Policy Statement	2

2.1 We are committed to being transparent when processing Personal Data and to implementing data protection by design and by default during the full lifecycle of our data processing activities. This includes applying appropriate safeguards during the collection, storage, processing and destruction of Personal Data.

3	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 Personal Data we process as a Data Controller and Personal Data we process as a processor (on behalf of our customers – if applicable).

3.2 Polyco Healthline Limited is registered in the UK as a Data Controller with the Information Commissioner's Office ("ICO"), registration number Z1836501.

4	Responsibilities	2

4.1 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 (Head of Digital and Technology Solutions, Head of HR and IT service and Infrastructure 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;
- Project owners are required to ensure that data protection by design and by default (as fully described in Section 6 of this Policy) is applied to new and existing business practices, processes, IT systems and technologies that involve the processing of Personal Data for which they are responsible.
- Project owners are required to carry out a Data Protection Impact Assessment ("DPIA") where the risks to Data Subjects associated with a data processing activity carried out by us as a Data Controller are high or where otherwise required by Section 7 of this Policy, and in such instances shall only process the Personal Data in question as permitted by the outcome of the DPIA.
- all personnel are required to read, understand and adhere to this Policy when processing Personal Data on our behalf.

4.2 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.

5	Data Protection by Design & Default Principles	3

5.1 The following data protection by design and by default principles shall apply to all Personal Data processed by us:

- **Preventative data protection**
  The rights of Data Subjects and their privacy shall be protected using proactive rather than reactive measures that anticipate risks to Data Subjects before they arise.

- **Data protection embedded by design**
  Measures to ensure data protection and to reduce risks to Data Subjects shall be embedded into the design and architecture of business practices and IT systems from the ground-up as part of their core functionality, rather than addressed later.

- **Data protection by default**
  Risks to Data Subjects associated with Personal Data processing shall be managed using default protection in business practices and IT systems which are proportionate to the likelihood and severity of the risks.

- **Transparent processing activities**
  Processing activities shall be transparent, whatever the business practices, processes or technology involved, and all processing shall be performed according to the privacy notices provided to Data Subjects and be subject to verification.

- **End-to-end data protection**
  Appropriate measures shall be implemented to ensure the rights of Data Subjects and their privacy are protected, and risks to Data Subjects are managed, from the collection of Personal Data throughout the full lifecycle of the data involved to the point of disposal.

- **Risk led data protection**
  The processing of Personal Data shall always take account of the risks to rights and freedoms of Data Subjects, and data protection impact assessments shall be carried out to evaluate the severity of that risk and to determine appropriate measures to mitigate the risk where processing is likely to result in a high risk to Data Subjects, or where otherwise required by law, the ICO, or this Policy.

5.2 Where we are the Data Controller, these principles shall govern all Personal Data processing. Applying data protection by design and by default and carrying out DPIAs will assist us to meet our data protection legal obligations and to build a relationship of trust with Data Subjects.

6	Data Protection by Design & Default	4

6.1 We shall ensure that the risks to rights and freedoms of Data Subjects associated with processing are key considerations when:

- designing, implementing and during the life of business practices and processes that involve the processing of Personal Data ("processing activities"); and
- 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").

6.2 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 individuals.

6.3 Where we are a Data Controller and the risks to rights and freedoms of Data Subjects is likely to be high, or where otherwise required by law or the ICO, a DPIA shall be performed as set out in Section 7 of this Policy.

6.4 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:

- data minimisation;
- limiting the extent of the processing, storage and access to what is strictly necessary;
- ensuring transparency for Data Subjects regarding the processing activities; and
- ensuring the security of the Personal Data.

6.5 Examples of common IT systems and technologies used in the processing of Personal Data are provided at Schedule 1 of this Policy.

7	Data Protection Impact Assessments	4-5

7.1 <u>Polyco Healthline as a Controller</u>

7.1.1 We will carry out a DPIA before or when we plan to carry out any of the following activities as a Data Controller:

- undertake any type of processing which is likely to result in a high risk to the rights and freedoms of Data Subjects;
- use systematic and extensive profiling based on automated processing with legal or similar significant effects on Data Subjects;
- process special category or criminal offence data on a large scale;
- systematically monitor publicly accessible places on a large scale; or
- undertake any other processing activity in a country in which the ICO has mandated that the processing activity necessitates a DPIA.

7.1.2 DPIAs shall be undertaken as set out in our DPIA Procedure and 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.

8	Implementation & Policy Management	5

8.1 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.

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

Signature:		**Place of Issue:**	Bourne, PE10 0DN, UK
Name:	Jack Prichard	**Date:**	17th March 2023
Position:	Deputy Chief Executive Officer		