Data Protection Policy

Company Policy No: 5
Company: Mayday Healthcare Ltd
Issue No: 10
Revision Date: April 2026
Review Date: April 2027

Data Protection Policy

Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Company name: Mayday Healthcare

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): either of the following:

a. the person required to be appointed in specific circumstances under the UK GDPR; or
b. where a mandatory DPO has not been appointed, a data privacy manager or other voluntary appointment of a DPO or the Company data privacy team with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards

specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Guidelines: the Company privacy and UK GDPR-related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available on our Wiki.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

a. general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or
b. stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on our Wiki.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Introduction

This policy and other documents referred to in it sets out the basis on which we will process any personal data that we collect from Data Subjects, or that is provided to us by Data Subjects or other sources.
This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the Company and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies and Privacy Guidelines.

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy has been written in line with the GDPR, effective 25th May 2018. The GDPR sets out the legal bases for processing data. For the purpose of this policy the company is a "data controller". The GDPR also gives individuals rights regarding their personal data including:

- The right to be informed
- The right to correction
- The right to access
- The right to object
- The right to restrict processing
- The right to erasure
- The right to data portability
- Rights regarding automation

In order to manage our business, we keep records about our employees that include the following. Please note this list is not exhaustive and can be changed:

- Full name
- Gender
- Date of birth
- Address
- Emergency contact information
- References
- Appraisals
- Qualifications
- CV's
- Bank details
- Right to work information
- Criminal record checks (where necessary)
- Sickness record
- Health information
- Disciplinary record

- Proof of employment i.e. service agreement
- CCTV imaging where applicable*

We will process data about our staff for legal reasons, because we have a legitimate business interest to do so or for the performance of a contract.

Under GDPR some data is referred to as sensitive personal data and this refers to data such as the following:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Health data
- Sexual orientation
- Criminal conviction data
- CCTV imaging where applicable*

We may process sensitive personal data relating to staff including, as appropriate:

- Information about any employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness to work.
- CCTV imaging*

We need explicit consent from an employee in order to process their sensitive data, and if consent is given it can be withdrawn easily.

**For further information on the CCTV that the business uses, please refer to our CCTV Policy.*

Our obligations

The six principles for processing personal data under GDPR are:

- Personal data should be processed fairly, lawfully and in a transparent manner
- Data should be obtained for specific and lawful purposes and not further processed in a matter incompatible with those purposes
- The data should be adequate, relevant and not excessive
- The data should be accurate and where necessary kept up to data
- Data should not be kept for longer than necessary
- Data should be kept secure

We are committed to following these principles and we ensure that all processing of data of which you are the subject is lawful. We will process data about you only as far as is necessary for the purpose of managing our business. Data will not be disclosed to anyone else other than our authorised employees, agents, contractors or advisors (except as required by law) unless you expressly authorise its disclosure. We will only obtain data about you that we require for the purpose of managing our business and dealing with you as an employee of that business.

We will take all reasonable steps to ensure that the data we process is accurate. Data will be retained as necessary during the course of your employment and we will follow all statutory retention periods. We will process data in accordance with your rights under GDPR.

Data will be kept in a secure system whether manual or computerised to the best of our ability at all times.

We will not disclose your data to a third party without your consent unless we are satisfied that they are legally entitled to the information. If your data is disclosed to a third party, we will ensure it still follows the six GDPR principles.

Our policy on access to data

- We have appointed a data protection officer
- On receipt of a request we will provide all data that we are obliged to disclose within 30 days of receipt of your request being received
- Should you wish to bring any inaccuracy in disclosed data to our attention, you are required to do so in writing
- We will ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken.

Where we have requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not be disclosed to you, it is our policy that it is unreasonable to disclose the reference to you, unless consent is obtained from the person who gave the reference.

Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Team at:

18th Floor
The Broadgate Tower
20 Primrose Street
London
EC2A 2EW

Chris Coyle
Director

Signed: 

Date: April 2026