DATA PROTECTION POLICY

Medic Now
Data protection policy

1 Introduction

This Data Protection Policy sets out how we, Medic Now, handle the personal data of our customers, suppliers, employees, workers, agency workers and other third parties.

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 our employees, workers, agency workers, interns, volunteers, apprentices and contractors.

You must read, understand and comply with this Data Protection Policy when processing personal data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you for us to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. 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, and conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the related policies and guidelines.

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

2 Interpretation

Definitions

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

2.1.2 **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.

2.1.3 **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 UK Data Protection legislation. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our commercial purposes.

2.1.4 **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.

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

2.1.6 **Data Protection Officer (DPO):** the person required to be appointed in specific circumstances under the UK GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or another voluntary appointment of a DPO or refers to the Company data privacy team responsible for data protection compliance.

2.1.7 **EEA:** the 27 countries in the EU, and Iceland, Liechtenstein and Norway.

Medic Now
Data protection policy

2.1.8 **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.

2.1.9 **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 our third-party service providers or we put in place to protect it. The loss, or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

2.1.10 **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.

2.1.11 **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.

2.1.12 **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, and biometric or genetic data.

3 Scope

3.1 All of our business and staff are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.2 The DPO is responsible for overseeing this Data Protection Policy. That post is held by the Data Protection Officer, who is contactable by email at dpo@yourworld.com.

3.3 Company Personnel must always contact the DPO in the following circumstances:

- **3.3.1** If you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Company)
- **3.3.2** If you need to rely on Consent and/or need to capture Explicit Consent
- **3.3.3** If you need to draft Privacy Notices
- **3.3.4** If you are unsure about the retention period for the Personal Data being Processed
- **3.3.5** If you are unsure about what security or other measures you need to implement to protect Personal Data
- **3.3.6** If there has been a Personal Data Breach
- **3.3.7** If you are unsure on what basis to transfer Personal Data outside the EEA
- **3.3.8** If you need any assistance dealing with any rights invoked by a Data Subject
- **3.3.9** Whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes other than what it was collected for
- **3.3.10** If you plan to undertake any activities involving Automated Processing, including profiling or Automated Decision Making; if you need help complying with applicable law when carrying out direct marketing activities
- **3.3.11** If you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors)

Medic Now
Data protection policy

4 Personal data protection principles

4.1 We adhere to the principles relating to the Processing of Personal Data set out in UK Data Protection Legislation which require Personal Data to be:

- **4.1.1** Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)
- **4.1.2** Collected only for specified, explicit and legitimate purposes (Purpose Limitation)
- **4.1.3** Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation)
- **4.1.4** Accurate and, where necessary, kept up to date (Accuracy)
- **4.1.5** Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation)
- **4.1.6** Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality)
- **4.1.7** Not transferred to another country without appropriate safeguards being in place (Transfer Limitation)
- **4.1.8** Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5 Lawfulness, fairness and transparency

5.1 Lawfulness and fairness:

5.1.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject

5.1.2 You may only collect, Process and share Personal Data for specified purposes. UK Data Protection Legislation restricts our actions regarding Personal Data to specified lawful purposes

5.1.3 UK Data Protection Legislation allows Processing for specific purposes, some of which are set out below:

- **5.1.3.1** The Data Subject has given his or her Consent
- **5.1.3.2** The Processing is necessary for the performance of a contract with the Data Subject
- **5.1.3.3** To meet our legal compliance obligations
- **5.1.3.4** To protect the Data Subject's vital interests
- **5.1.3.5** To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices

5.1.4 If you are processing special category information, you will require an additional lawful basis

5.1.5 You must identify and document the legal ground being relied on for each Processing activity. If you are unsure of the lawful basis, please contact the Data Protection Officer

5.2 Consent

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

Medic Now
Data protection policy

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

Data Subjects must be easily able to withdraw Consent to Processing at any time, and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose from the original purpose.

You will need to evidence Consent captured and keep records of all Consent so the Company can demonstrate compliance with Consent requirements.

5.3 Transparency (notifying data subjects):

UK Data Protection Legislation requires Data Controllers to provide detailed, specific information to Data Subjects. Such information must be provided through appropriate Privacy Notices, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK Data Protection Legislation and relevant standards to protect Personal Data.

6 Transfer limitation

UK Data Protection Legislation restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK Data Protection Legislation is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may not transfer information outside the UK or EEA unless prior authorisation has been sought. If you believe that you need to seek authorisation to transfer information outside of the UK or EEA, please contact the Data Protection Officer immediately and before the transfer takes place.

7 Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the date is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

Medic Now will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for minimum time.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we longer require in accordance with our applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Medic Now
Data protection policy

8 Accountability

8.1 Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to understand and comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training. You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

8.2 Record keeping

UK Data Protection Legislation requires us to keep full and accurate records of all our data Processing activities.
You must keep and maintain accurate corporate records reflecting our Processing, including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

8.3 Data Protection Impact Assessment (DPIA)

8.3.1 Data controllers must conduct DPIAs with respect to high risk Processing.

8.3.2 You should conduct a DPIA (and discuss your findings with the Data Protection Officer) when implementing major system or business change programs involving the Processing of Personal Data, including:

- **8.3.2.1** Use of new technologies (programs, systems or processes) or changing technologies (programs, systems or processes)
- **8.3.2.2** Automated Processing, including profiling and ADM
- **8.3.2.3** Large scale Processing of Special Categories of Personal Data or Criminal Convictions Data
- **8.3.2.4** Large scale, systematic monitoring of a publicly accessible area

A DPIA must include:

- **8.3.2.5** A description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate
- **8.3.2.6** An assessment of the necessity and proportionality of the Processing in relation to its purpose
- **8.3.2.7** An assessment of the risk to individual
- **8.3.2.8** The risk mitigation measures in place and demonstration of compliance

8.3.3 If you believe that a DPIA is required, please contact the Data Protection Officer immediately and before the project/ change begins

8.4 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers under the Privacy and Electronic Marketing Regulation.

You must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Medic Now
Data protection policy

For example, a Data Subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers, known as "soft opt-in", allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

8.5 Sharing personal data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

A. They have a need to know the information for the purposes of providing the contracted services

B. Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained

C. The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place

D. The transfer complies with any applicable cross border transfer restrictions

E. A fully executed written contract that contains GDPR approved third party clauses has been obtained

9 Security, integrity and confidentiality

9.1 Protecting personal data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness or those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Criminal Convictions Data from loss and unauthorised access, use or disclosure.

Medic Now
Data protection policy

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

F. Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it

G. Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed

H. Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes

9.2 Reporting a personal data breach

UK Data Protection Legislation requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach. We will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

10 CCTV

We use closed-circuit television (CCTV) images. There is no audio recording, i.e., conversations are not recorded on the Company's CCTV.

Cameras are located at strategic points throughout the Company's business premises, principally with the entrance and exit points and within our communal areas. All cameras are clearly visible, and appropriate signs are prominently displayed so that employees, clients and other visitors are aware that they are being monitored when entering our premises.

11 Changes to this data protection policy

We reserve the right to change this Data Protection Policy at any time, so please check back regularly to obtain the latest copy of this Data Protection Policy.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

Should you require any information about the information in this or any other data protection related policy, please contact the Data Protection Officer by emailing *dpo@youworld.com*.