



MEDICORP

YOUR HEALTHCARE PARTNER

Data Protection Policy

Privacy Policy

Data Controller: Medicorp

Contact: admin@medicorpmalta.com

Version 1.0 | August 2024

Table of Contents

1. Introduction and Purpose	3
2. Scope	3
3. Who We Are – the Data Controller	3
4. Definitions	3
5. Data Protection Principles	3
6. Categories of Personal Data We Process	4
7. How We Obtain Personal Data	4
8. Purposes of Processing	4
9. Our Lawful Bases for Processing	4
10. Processing of Health (Special Category) Data	5
11. Disclosure of Personal Data and Recipients	5
12. Data Storage and International Transfers	5
13. Data Security	6
14. Data Retention	6
15. Your Data Protection Rights	6
16. Automated Decision-Making and Profiling	7
17. Data Protection Officer	7
18. How to Contact Us and Raise Concerns	7
19. Right to Lodge a Complaint	7
20. Changes to This Policy	7

1. Introduction and Purpose

Medicorp (“Medicorp”, “the Company”, “we”, “us” or “our”) is committed to protecting the privacy and security of the personal data it processes. This Data Protection Policy explains how the Company collects, uses, discloses, stores and protects personal data in connection with its medical sick-leave verification and related services, and sets out the rights available to the individuals whose personal data we process.

The Company processes personal data in accordance with Regulation (EU) 2016/679 (the General Data Protection Regulation, or “GDPR”), the Data Protection Act (Chapter 586 of the Laws of Malta) and any subsidiary legislation made thereunder (together, “Data Protection Law”).

2. Scope

This Policy applies to all personal data processed by the Company in the course of providing its services, including the personal data of: (a) the individuals who are the subject of a medical sick-leave verification or assessment (the “individuals assessed” or “data subjects”); and (b) the representatives and contact persons of the Company’s customers. It applies to processing carried out by electronic means and to personal data held in a structured manual filing system.

3. Who We Are – the Data Controller

For the purposes of Data Protection Law, Medicorp is the controller of the personal data described in this Policy. This means that the Company determines the purposes and the means of the processing of that personal data – including the manner in which health-related data is processed – and is responsible for ensuring that the processing complies with Data Protection Law.

Contact details: Medicorp – Email: admin@medicorpmalta.com

4. Definitions

In this Policy:

- **“Personal data”** means any information relating to an identified or identifiable natural person.
- **“Special categories of personal data”** include data concerning health, which benefits from additional protection under Data Protection Law.
- **“Processing”** means any operation performed on personal data, such as collection, recording, storage, use, disclosure or erasure.
- **“Controller”** means the party that determines the purposes and means of processing.
- **“Processor”** means a party that processes personal data on behalf of the controller.

5. Data Protection Principles

The Company adheres to the data protection principles set out in Data Protection Law. Personal data is: processed lawfully, fairly and in a transparent manner; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary (data minimisation); accurate and, where necessary, kept up to date; kept in a form that permits identification for no longer

than is necessary (storage limitation); and processed in a manner that ensures appropriate security (integrity and confidentiality). The Company is responsible for, and able to demonstrate, its compliance with these principles (accountability).

6. Categories of Personal Data We Process

In the course of providing its sick-leave verification services, the Company processes the following categories of personal data:

- **Identification and contact data of the individual to be assessed** – including full name, identity card or document number, and residential address – as provided to us by our customer.
- **Health-related data (special category data)** – the outcome of the medical assessment carried out by the attending medical practitioner, including information relating to the individual's fitness or ability to work and the expected date of return to work.
- **Customer contact data** – the names, job titles and contact details of the representatives of our customers who instruct us.

The Company does not seek to collect more personal data than is necessary for the purposes described in this Policy.

7. How We Obtain Personal Data

The Company obtains personal data:

- From its customers, who provide the identification and contact details of the individuals to be assessed when instructing the Company; and
- From the medical practitioners engaged to carry out the assessment, who provide the results of the assessment to the Company.

The individuals assessed do not usually provide their personal data to the Company directly.

8. Purposes of Processing

The Company processes personal data for the following purposes:

- To arrange and coordinate the medical sick-leave verification visits and assessments requested by our customers;
- To share the necessary identification and contact details with the medical practitioner who will carry out the visit;
- To receive, review and securely store the results of the assessment;
- To prepare and provide a report to the customer confirming the outcome relevant to the customer – namely the date on which the individual is expected to return to work – without disclosing the underlying medical data;
- To respond to queries, manage our relationship with customers and keep proper records; and
- To comply with our legal obligations and to establish, exercise or defend legal claims.

9. Our Lawful Bases for Processing

The Company relies on the following lawful bases under Article 6(1) GDPR:

- **Legitimate interests (Article 6(1)(f))** – the processing is necessary for the legitimate interests of the Company and of its customers in verifying sickness absence and in the proper management of workplace attendance, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual; and
- **Contract and legal obligation (Article 6(1)(b) and (c))** – in relation to our dealings with customer contacts and to comply with obligations to which the Company is subject.

Because the assessment involves data concerning health, the Company also relies on a condition under Article 9(2) GDPR, as set out in Section 10.

10. Processing of Health (Special Category) Data

Data concerning health is a special category of personal data that benefits from additional protection. The Company processes health data only to the extent necessary to provide its services and relies on one or more of the following conditions under Article 9(2) GDPR:

- **Article 9(2)(h)** – processing is necessary for the assessment of the working capacity of the individual, carried out by or under the responsibility of a health professional who is subject to the obligation of professional secrecy;
- **Article 9(2)(b)** – processing is necessary for the purposes of carrying out obligations and exercising rights in the field of employment law, in so far as it is authorised by law; and/or
- **Article 9(2)(a)** – the explicit consent of the individual, where the Company relies upon it.

The Company applies the following additional safeguards to health data:

- Health data is treated as strictly confidential and access is restricted to those who genuinely need it to perform their duties;
- Health data is not included in the report provided to the customer – the report communicates only the outcome required by the customer, namely the individual's expected date of return to work;
- Health data is kept undisclosed and stored securely, separately from the reports issued to customers; and
- Health data is retained only for as long as necessary and is then securely deleted.

11. Disclosure of Personal Data and Recipients

The Company discloses personal data only as necessary to provide its services and as permitted by Data Protection Law. Recipients may include:

- **Medical practitioners** engaged to carry out the assessment, who receive the individual's name, identity number and address in order to conduct the visit;
- **Our customer**, who receives a report confirming the individual's expected date of return to work and does not receive the individual's underlying medical data; and

- **Third-party service providers** who process personal data on our behalf, such as secure cloud storage providers, and who are bound by appropriate confidentiality and data-processing obligations.

The Company does not sell personal data and does not disclose it for marketing purposes. Personal data may be disclosed where the Company is required to do so by law or in response to a valid request from a competent authority.

12. Data Storage and International Transfers

Personal data is stored on the Company's systems and using reputable third-party cloud services, which the Company currently uses for secure storage and for the collection of assessment data – including services such as Apple iCloud and Google (Google Forms). Some of these providers may store or process personal data on servers located outside Malta and, in certain cases, outside the European Economic Area (EEA).

Where personal data is transferred outside the EEA, the Company ensures that an appropriate safeguard recognised under Data Protection Law is in place – such as an adequacy decision of the European Commission, the European Commission's Standard Contractual Clauses, or another lawful transfer mechanism – so that the personal data continues to benefit from an adequate level of protection.

13. Data Security

The Company implements appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures include restricting access to personal data to authorised personnel on a need-to-know basis; the use of access controls and passwords; the use of reputable and secured storage services; keeping health data undisclosed and segregated from the reports issued to customers; and ensuring that personnel are aware of their confidentiality obligations. The Company keeps its security measures under review.

14. Data Retention

The Company retains personal data only for as long as is necessary to fulfil the purposes for which it was collected, including to provide the service, to respond to any related queries, and to comply with any legal, accounting or reporting obligations. Health-related assessment data is retained only for as long as necessary and, as a default, is securely deleted within 12 months of completion of the assessment, unless a longer period is required by law or is necessary for the establishment, exercise or defence of legal claims. When personal data is no longer required, it is securely deleted or anonymised.

15. Your Data Protection Rights

Subject to the conditions and exceptions provided under Data Protection Law, individuals have the following rights in relation to their personal data:

- The right to be informed about how their personal data is processed;

- The right of access to their personal data;
- The right to rectification of inaccurate or incomplete personal data;
- The right to erasure (the “right to be forgotten”) in certain circumstances;
- The right to restrict processing in certain circumstances;
- The right to data portability in certain circumstances;
- The right to object to processing based on the Company’s legitimate interests; and
- Where processing is based on consent, the right to withdraw that consent at any time, without affecting the lawfulness of processing carried out before the withdrawal.

To exercise any of these rights, please contact us using the details in Section 18. We will respond within the timeframes set out in Data Protection Law. Exercising these rights is generally free of charge, although we may charge a reasonable fee or decline to act where a request is manifestly unfounded or excessive, as permitted by law. We may need to verify your identity before acting on a request.

16. Automated Decision-Making and Profiling

The Company does not take decisions that produce legal effects concerning an individual, or that similarly significantly affect an individual, based solely on automated processing, including profiling.

17. Data Protection Officer

The Company has designated a point of responsibility for data protection matters. Where the appointment of a Data Protection Officer (DPO) is required under Data Protection Law, the DPO may be contacted at admin@medicorpmalta.com. The role of the DPO includes monitoring the Company’s compliance with Data Protection Law and acting as a contact point for data subjects and for the supervisory authority.

18. How to Contact Us and Raise Concerns

If you have any questions about this Policy, wish to exercise any of your rights, or have any concern about how the Company processes personal data, please contact us at:

Medicorp

Email: admin@medicorpmalta.com

We take all concerns seriously and will do our best to resolve them.

19. Right to Lodge a Complaint

If you are not satisfied with how the Company has handled your personal data or a request you have made, you have the right to lodge a complaint with the supervisory authority in Malta:

Office of the Information and Data Protection Commissioner (IDPC)

Floor 2, Airways House, High Street, Sliema SLM 1549, Malta

Telephone: +356 2328 7100

Email: idpc.info@idpc.org.mt

Website: idpc.org.mt

20. Changes to This Policy

The Company may update this Policy from time to time to reflect changes in its practices or in the applicable law. The current version and its effective date are shown on the title page of this document. Where changes are material, the Company will communicate them as appropriate.