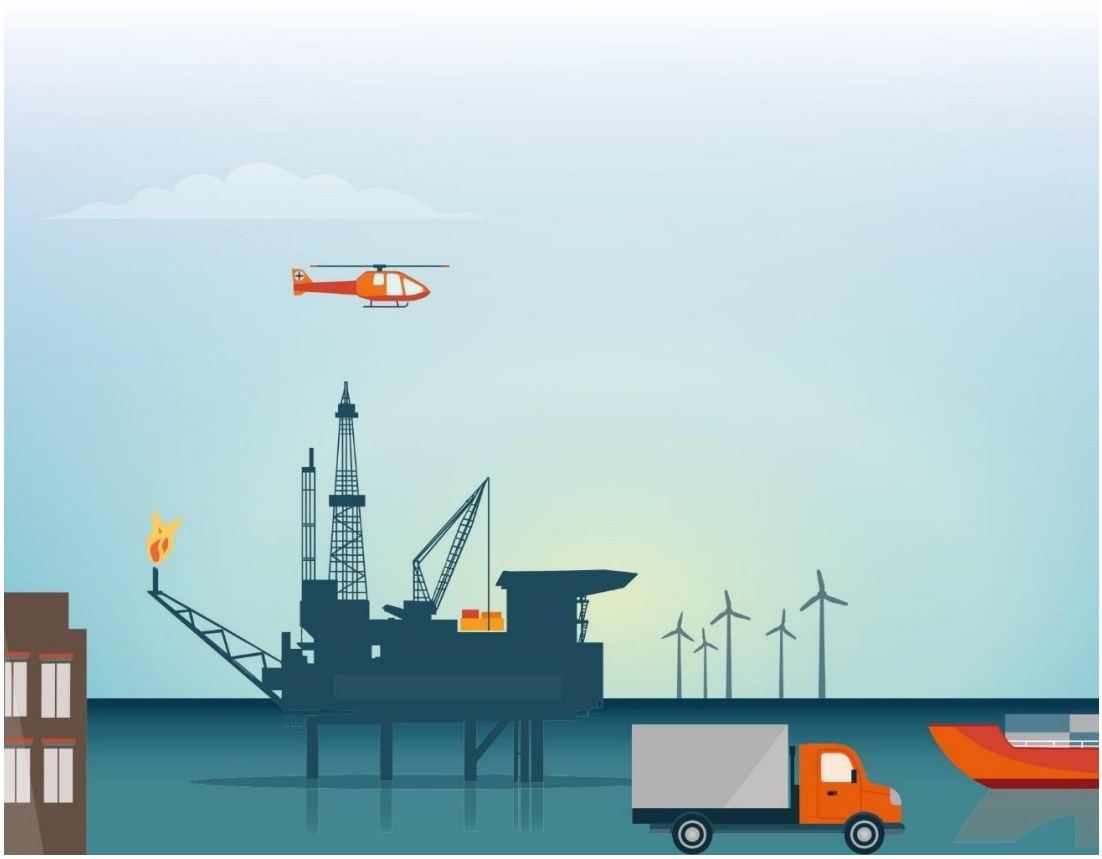
Privacyregulations MediWerk B.V.



Version 4.3 – January 2026
Classification: C1-Public
Approval: Peter Mijnster
Prepared by: Katja van Mil, Jeanet de Zeeuw, Peter Mijnster

Welkom to MediWerk

We are here to support employers and employees in optimizing health, safety and sustainable employability. At MediWerk B.V. (hereinafter: MediWerk), we handle personal data with the utmost care and respect for privacy. Our Data Protection Officer ensures that we comply with all applicable laws and regulations, including the GDPR. We only collect data that is necessary for carrying out our tasks, including our legal obligations.

Contents

1 | Purpose, status and scope

MediWerk B.V. processes personal data, including special categories of personal data and in particular health data, in the context of its occupational health services, occupational medical services, absence management, reintegration, preventive services, medical examinations, periodic examinations, advisory activities and supporting processes.

These privacy regulations describe, per registration, how MediWerk records, uses, secures, makes available, discloses and retains personal data. The purpose of this document is to clearly inform clients, customers, employees and other data subjects about how MediWerk handles personal data and how statutory rights can be exercised.

These privacy regulations have been drawn up in conjunction with the General Data Protection Regulation, the GDPR Implementation Act, the Working Conditions Act, the Medical Treatment Contracts Act, the Individual Healthcare Professions Act, relevant KNMG and NVAB guidelines, the Certification Scheme for Occupational Health Services, and MediWerk's internal privacy, information security and complaints documentation.

MediWerk applies one overarching set of privacy regulations with a clear elaboration per registration. This keeps the regulations practical and manageable, while ensuring that the minimum required subjects are described for each registration.

2 | Definitions

For the purposes of these regulations, the following definitions apply:

- **Personal data:** All information relating to an identified or identifiable natural person.
- **Special categories of personal data:** Personal data that requires additional protection due to its nature, including health data.
- **Processing:** Any operation or set of operations performed on personal data, such as collection, recording, organization, storage, consultation, use, disclosure, restriction, deletion or destruction.
- **Registration:** A coherent set of personal data within a specific process, purpose or information system of MediWerk.
- **Client:** The natural person to whom the service or processing relates, including employees, examinees, participants in examinations, consumers or other natural persons concerned.
- **Customer:** The employer, principal or other contractual relationship of MediWerk.
- **Controller:** MediWerk B.V., insofar as MediWerk determines the purpose of and means for the processing.
- **Processor:** An external party that processes personal data on behalf of MediWerk.
- **Physician / Occupational Physician / Examining Physician:** The physician who, by virtue of his or her professional role, is involved in medical assessment, guidance or advice.
- **Absence and Reintegration Team:** The persons involved under the responsibility of the occupational physician in absence management and reintegration, including case management and supporting medical or administrative roles where necessary.
- **Data Protection Officer:** The officer appointed by MediWerk who independently supervises compliance with privacy legislation.
- **Medical Record:** The record in which medical personal data of a client, and personal data directly related thereto, are stored.
- **Consent:** Any freely given, specific, informed and unambiguous indication of the client's wishes by which the client agrees to a specific processing or disclosure of personal data, where consent is the appropriate legal basis or additional requirement.

3 | Legal framework and principles

MediWerk processes personal data solely for legitimate, specific and clearly defined purposes. The following principles apply:

- personal data is processed only insofar as necessary for the purpose of the registration;
- MediWerk does not process more personal data than necessary;
- access is granted on a need-to-know basis and through role-based authorization;
- medical personal data is processed only by or under the responsibility of persons who are authorized to do so by virtue of their role or legal position;
- disclosure to customers or third parties takes place only where there is a legal basis or, where required, where the client's specific consent has been obtained;
- consent is demonstrably recorded in the file or in the designated systems or forms;
- data subjects can exercise their statutory rights in accordance with the procedure described in these regulations;
- personal data is not retained longer than necessary or legally required;
- personal data is protected by appropriate technical and organizational measures.

MediWerk does not use automated decision-making or profiling with significant effects for clients without human intervention.

4 | Registrations within MediWerk

Within these privacy regulations, MediWerk distinguishes the following registrations:

- absence management and reintegration registration;
- medical record-keeping and occupational medical guidance registration;
- PAGO/PMO and other occupational health examination registration;
- medical examinations registration;
- prevention and working conditions registration;
- planning, intake, contact and client communication registration;
- customer and assignment file registration at organizational level;
- website, form and supporting customer contact data registration.

For each registration, at least the purpose, origin, access, authorization management, client rights, disclosure to third parties and consent requirements are described in these regulations and annexes.

5 | General rules for access and authorization management

5.1 | Need-to-know and role-based access

Access to personal data is always granted on a need-to-know basis. This means that only those persons who require the data for the performance of their duties are given access.

A stricter regime applies to medical personal data. Access to medical content is limited to physicians and other persons involved under the responsibility of the physician or occupational physician in the performance of the relevant service, insofar as such access is necessary.

5.2 | Granting authorizations

Authorizations are granted on the basis of role, function, process responsibility and system use. The manager and, where relevant, the process owner or system owner determine which access is necessary. Functional management and IT implement the authorization technically in the designated systems.

5.3 | Management and amendment of authorizations

Authorizations are managed through a fixed process for onboarding, role changes, temporary replacement, external engagement and offboarding. Changes in access are recorded and, where required, approved. Conflicting or unnecessary authorizations are removed.

5.4 | Review of authorizations

MediWerk performs periodic checks on access rights, authentication logs and relevant administrative actions. Where necessary, authorizations are adjusted. Upon termination of activities, access rights are withdrawn as soon as possible.

5.5 | IT and functional management

IT management and functional management only have access for management, support, maintenance and continuity purposes, insofar as necessary. This access is not intended for substantive processing or assessment of client data. Where possible, substantive access is technically restricted, logged or shielded.

5.6 | Quality review and supervision

Senior professionals, staff physicians or other designated experts may have access to records for quality purposes, peer review, supervision or professional support, insofar as this is necessary within their field of expertise and responsibility.

6 | Exercise of rights by clients and other data subjects

Clients and other data subjects may exercise their statutory rights under the GDPR, including the rights referred to in Articles 15 through 22 GDPR, insofar as applicable in the specific situation. These include:

- the right to information;
- the right of access;
- the right to rectification;
- the right to erasure, insofar as legally possible;
- the right to restriction of processing;
- the right to data portability, where applicable;
- the right to object;
- rights relating to automated decision-making and profiling, where applicable.

6.1 | Submitting a request

A request may be submitted in writing or electronically via MediWerk's contact channels. MediWerk may request additional identification or verification in order to establish that the request originates from the correct person.

6.2 | Handling

MediWerk registers the request, assesses the applicability of the requested right and responds within the statutory period. If a request is rejected in whole or in part, MediWerk provides written reasons.

6.3 | Medical records

Where a request relates to medical personal data or a medical record, the assessment and handling take place with due regard for the applicable medical and professional legal frameworks.

6.4 | Copies and transfer

Clients may request a copy of their personal data or, where applicable, transfer of data. MediWerk only provides data in a secure and appropriate manner.

7 | Disclosure to third parties and consent

7.1 | General rule

Personal data from a registration is disclosed to third parties or to the customer only if there is a legal basis for doing so or if the client has given specific consent, insofar as consent is required.

7.2 | Medical personal data

Specific written consent from the client is required for the disclosure of medical personal data to the customer or to third parties, unless a specific legal obligation or legal exception applies. Such consent is recorded in the medical record or in another demonstrable manner traceable to the relevant client, disclosure and date.

7.3 | Consultation of the occupational physician and voluntary examinations

No information is provided to the customer or third parties regarding a consultation of the occupational physician by the client or the client's voluntary participation in periodic examinations. If, following such consultation or examination, the occupational physician wishes to provide advice to the customer regarding the client's working conditions or employability, the client's verbal consent is required. This verbal consent is demonstrably recorded in the medical record.

7.4 | Recording consent

Depending on the situation, consent is recorded by means of:

- a signed written consent form;
- digital recording in the medical record or source system;
- a scan or digital copy of a signed form;
- an explicit file note of verbally given consent, including date, context and scope;
- a recorded authorization for file transfer or information request.

For disclosure of medical personal data to the customer or to third parties, specific written consent of the client is recorded, unless a legal obligation or legal exception applies. In situations where the occupational physician wishes to provide advice to the customer following a consultation or voluntary periodic examination, the client's verbal consent is demonstrably recorded in the medical record.

7.5 | Taking note of disclosures to third parties

Clients may request information from MediWerk about whether and, insofar as permitted, to which third parties personal data from a registration has been disclosed. MediWerk assesses such a request within the applicable legal and professional frameworks.

8 | Retention periods and destruction

MediWerk does not retain personal data longer than necessary for the purpose of the registration, unless a longer retention period follows from laws and regulations, the duty of care of a good healthcare professional, ongoing proceedings, or a justified need to demonstrate rights or obligations.

8.1 | Main principles

- medical records and occupational medical records are, in principle, retained in accordance with the applicable medical retention obligations;
- data from medical examinations is retained for as long as necessary for the purpose of the examination and in accordance with applicable laws and regulations;
- data relating to exposure to hazardous substances or ionizing radiation is retained in accordance with the applicable longer statutory retention periods;
- personnel files, application data, website data and supporting contact data follow the separately applicable retention periods and procedures;
- once a retention period has expired and there is no valid reason for further retention, data is securely deleted or destroyed.

8.2 | Transfer when changing occupational health service provider or physician

If a customer switches to another occupational health service provider or occupational physician, MediWerk assesses which data must be transferred based on law, professional standards, continuity of guidance and consent or request of the client. The transfer takes place securely and in a controlled manner.

9 | Security of personal data

MediWerk takes appropriate technical, organizational and procedural measures to protect personal data against loss, unauthorized access, unlawful processing, unwanted alteration and unauthorized disclosure.

These measures include, among other things:

- role-based authorizations;
- multi-factor authentication where available and required;
- logging and monitoring of access;
- management of workplaces, systems and company assets;
- secure data exchange;
- backup and recovery measures;
- patch and update management;
- confidentiality obligations;
- instruction, awareness and training;
- appropriate contractual and organizational control of processors and suppliers.

MediWerk uses various systems and SaaS solutions for its services and support. For each system, access, configuration and use are controlled under MediWerk's responsibility insofar as may reasonably be expected of MediWerk.

10 | Complaints procedure

If a client, customer or other data subject believes that MediWerk is not correctly applying these privacy regulations, privacy legislation or the data subject's privacy rights, a complaint may be submitted in accordance with MediWerk's complaints procedure.

This reference also serves to meet the requirements of the Certification Scheme for Occupational Health Services. MediWerk's complaints procedure describes how complaints are submitted, registered, handled, followed up and resolved. This complaints procedure is available through MediWerk's usual communication channels and is provided free of charge upon request.

Submitting a complaint to MediWerk does not affect the right of a data subject to contact the Data Protection Officer or, where applicable, the Dutch Data Protection Authority.

11 | Availability of these privacy regulations

These privacy regulations are available to customers and clients via the MediWerk website as a downloadable document or are provided free of charge upon request. In this way, the privacy regulations are accessible to both customer and client in accordance with the requirements of the Certification Scheme for Occupational Health Services.

Where a public version is made available, MediWerk ensures that it provides sufficient insight into how personal data is processed and protected, without unnecessarily disclosing sensitive security details.

12 | Entry into force and management

These privacy regulations enter into force on the date of formal adoption by MediWerk and replace previous versions of privacy regulations insofar as they relate to the same registrations.

MediWerk reviews these privacy regulations periodically and in any event in the event of relevant changes in services, laws and regulations, processes, systems, registrations, risks or audit findings.

Annex 1 | Overview of registrations

Registration 1 | Absence management and reintegration

Purpose of the registration: Recording and using personal data necessary for guidance in case of sickness absence, reintegration, advice in the context of the Improved Gatekeeper Act, absence control, return to work, and related communication and follow-up.

Origin of the data: The data may originate from the client, the employer or principal, the occupational physician, other professionals involved in the guidance, previous occupational health service providers, treating professionals or other third parties insofar as legally permitted and, where required, after the client's specific consent.

Persons with access:

- occupational physician and physicians involved in the guidance;
- case managers and absence management staff insofar as necessary for their role;
- doctor's assistants and medically supporting staff insofar as necessary;
- senior professionals or staff physicians for quality purposes or supervision;
- planning or administration staff solely for process, appointment and contact data insofar as necessary;
- functional management and IT management solely for management and support, not for substantive assessment.

Authorization management: Authorizations are granted on the basis of role and necessity, approved through the regular authorization procedure and reviewed periodically.

Statutory rights of the client: The client may submit a request for access, rectification, copy, restriction, transfer or objection in accordance with Chapter 6 of these regulations.

Disclosure to third parties and consent: Only the data that may be shared within the legal framework of sickness absence management and reintegration is disclosed to the employer. Disclosure of medical personal data to the employer or other third parties takes place only with the client's specific consent, unless a legal obligation provides otherwise. Consent is recorded in the file.

Registration 2 | Medical record-keeping and occupational medical guidance

Purpose of the registration: Creating and maintaining a medical record and supporting medical assessment, treatment, guidance, consultation and professional accountability within occupational medical services.

Origin of the data: The data may originate from the client, the physician, examination results, medical correspondence, other healthcare providers or treating professionals, previous files or other occupational health service providers, insofar as the disclosure takes place lawfully and, where required, with the client's consent.

Persons with access:

- occupational physician, physician and examining physician insofar as involved;
- doctor's assistant or medical secretariat insofar as necessary for support;
- case manager only insofar as the role and legal frameworks permit;
- senior professional or staff physician for quality purposes or supervision;
- functional management and IT management solely for technical management, not for substantive processing.

Authorization management: Access to medical content is restricted and granted on the basis of explicit role assignment. Access rights are reviewed periodically and adjusted immediately where necessary.

Statutory rights of the client: The client may exercise the rights referred to in Chapter 6. Where the nature of medical record-keeping requires, MediWerk acts within the applicable medical and professional legal frameworks.

Disclosure to third parties and consent: Medical data is only disclosed to third parties or to the customer if there is a legal basis for doing so or if the client's specific consent has been obtained. Written or otherwise demonstrably recorded consent is included in the file.

Registration 3 | PAGO/PMO and other occupational health examinations

Purpose of the registration: Planning, carrying out, recording and reporting on periodic occupational health examinations, preventive medical examinations and related analyses, advice and follow-up.

Origin of the data: The data originates from the client, measurement and examination results, questionnaires, medical or occupational health assessments and, where relevant, from the employer at organizational level for the design of the examination.

Persons with access:

- occupational physician or other physicians for medical assessment;
- authorized medical or examination staff;
- planning and administration staff for necessary process and appointment data;
- senior professionals or quality staff for anonymized or necessary quality purposes;
- functional management and IT management solely for technical management.
- **Authorization management:** Authorizations follow the general rules of Chapter 5. Medical content remains shielded from persons who do not need that content.

Statutory rights of the client: The client may exercise the rights described in Chapter 6.

Disclosure to third parties and consent: Voluntary participation in periodic examinations is not disclosed to the customer or third parties. If, following an examination, individual advice is given to the customer, the client's verbal consent is required and is recorded in the medical record. Reports at organizational level are provided in aggregated or anonymized form where necessary.

Registration 4 | Medical examinations

Purpose of the registration: Planning, carrying out, recording and reporting on medical examinations, including pre-employment examinations and other examinations lawfully performed within MediWerk's services.

Origin of the data: The data originates from the client, questionnaires, examination results, medical examinations, observations of the examining physician and, where applicable, additional information from third parties obtained lawfully.

Persons with access:

- examining physician and other involved physicians;
- medically supporting staff insofar as necessary;
- planning and administration staff for appointment and contact data;
- senior professionals for quality and supervision;
- functional management and IT management solely for technical management.
- **Authorization management:** Authorizations are role-based and limited to what is necessary for the performance and support of the examination.

Statutory rights of the client: The client may exercise the rights described in Chapter 6.

Disclosure to third parties and consent: The outcome or feedback of an examination is only shared within the applicable legal and professional frameworks. Where medical personal data is disclosed to third parties, the client's specific consent is required unless a specific legal provision provides otherwise.

Registration 5 | Prevention and working conditions

Purpose of the registration: Recording and using personal data necessary for consultation, advisory services, workplace assessments, preventive guidance, working conditions support and related feedback.

Origin of the data: The data may originate from the client, the employer, the occupational physician, workplace assessments, RI&E-related information, other experts or observations in the context of the services.

Persons with access:

- occupational physician;
- higher safety expert, occupational hygienist, work and organizational expert or other experts insofar as involved and necessary;
- medical or administrative supporting roles insofar as necessary;
- senior professionals for quality purposes;
- functional management and IT management solely for technical management.

Authorization management: Authorization is limited to the persons who require access for their specific professional role.

Statutory rights of the client: The client may exercise the rights under Chapter 6.

Disclosure to third parties and consent: Individual medical information is not shared with the customer or third parties without specific consent. Advice at organizational level is, where possible, provided without identifiability to individual clients.

Registration 6 | Planning, intake, contact and client communication

Purpose of the registration: Planning appointments, maintaining contact, processing intake data, answering questions, supporting services and organizing client and customer communication.

Origin of the data: The data originates from the client, the customer, website or contact forms, telephone or written communication, internal recording and supporting systems.

Persons with access:

- planners and administrative staff insofar as necessary for their activities;
- physicians or other treating professionals insofar as the data is relevant to the services;
- customer contact or support staff insofar as necessary;
- functional management and IT management solely for technical management.

Authorization management: Access is limited to process and contact data and is not configured more broadly than necessary.

Statutory rights of the client: The client may exercise the rights under Chapter 6.

Disclosure to third parties and consent: Data is only shared with third parties or processors insofar as necessary for the performance of the services, secure communication or legal obligations. Where medical content is involved, the stricter rules of Chapter 7 apply.

Registration 7 | Customer and assignment file formation at organizational level

Purpose of the registration: Recording customer data, contractual agreements, contact persons, organizational-level advice, reports, service agreements and process information necessary for the performance and management of the relationship with the customer.

Origin of the data: The data originates from the customer, contact persons, MediWerk, contractual documentation, correspondence and operational services.

Persons with access:

- management and executive management insofar as necessary;
- account or relationship responsible staff;
- administrative and supporting staff insofar as necessary;
- involved experts insofar as relevant for performance of the assignment;
- functional management and IT management solely for technical management.

Authorization management: Authorizations are based on customer responsibility, process role and necessity.

Statutory rights of the client: Insofar as this registration contains personal data of natural persons, data subjects may exercise the rights under Chapter 6.

Disclosure to third parties and consent: Data from this registration is disclosed only insofar as necessary for contract performance, legal obligations, audit, insurance, financing or other legitimate business processes within the applicable legal framework.

Registration 8 | Website, forms and supporting customer contact data

Purpose of the registration: Processing contact requests, website submissions, questions, applications and other supporting customer or client contacts.

Origin of the data: The data originates from the data subject directly, via website, email, telephone, forms or other contact channels.

Persons with access:

- staff handling the relevant contact;
- planning, administration or support staff insofar as necessary;
- functional management and IT management solely for technical management.

Authorization management: Access is limited to those staff handling or supporting the contact or request.

Statutory rights of the client: Data subjects may exercise the rights under Chapter 6.

Disclosure to third parties and consent: Data is only shared if necessary for responding, carrying out the request, legal obligations or the engagement of processors. Special categories of personal data are not shared beyond what is necessary and only within the applicable legal framework.

Annex 2 | Functions and access roles

The following functions may, depending on their role and the relevant registration, have access to personal data:

- management and executive management insofar as necessary for governance, contractual responsibility, quality or legal duties;
- occupational physician, physician and examining physician;
- doctor's assistant, medical secretariat and other medically supporting staff;
- case manager, absence management staff and reintegration support staff;
- planners and administrative staff;
- higher safety expert, occupational hygienist, work and organizational expert and other experts;
- senior professionals, staff physicians and quality staff;
- functional management and IT management solely for technical and functional management;
- privacy, governance or compliance staff insofar as necessary for supervision, incident handling or lawful handling of requests.

Actual access is always determined by the registration, the nature of the data, the professional responsibility and the need-to-know principle.

Annex 3 | Guideline for recording consent

MediWerk records consent for the disclosure of medical personal data in a demonstrable manner. This is done in any case in one or more of the following ways:

- by including a signed consent form in the medical record;
- by digitally recording explicit consent in the medical record or the source system used;
- by including a file note with the date, content, recipient and scope of verbal consent;
- by including an authorization for file transfer or the request of medical information;
- by recording consent in the context of an occupational health consultation, periodic examination or consultation, insofar as the occupational physician wishes to provide advice to the customer on that basis.

The recording must be set up in such a way that it can be demonstrated afterwards:

- who gave consent;
- on what date consent was given;
- what the consent related to;
- to whom data could be disclosed;
- whether it concerned written or verbal consent;
- where the recording can be found.