Privacy Statement MediWerk B.V.

Version 2.0 – March 2024
Classification: C1-Public

Welcome to MediWerk

We are here to support employers and employees in optimizing health, safety, and sustainable employability. At MediWerk B.V. (hereafter MediWerk), we handle personal data with the utmost care and respect for privacy. Our Data Protection Officer ensures we comply with all applicable laws and regulations, including the GDPR. We only collect data necessary for performing our tasks, including legal obligations. In our privacy statement, we explain how we handle personal data and the rights and obligations arising from this. At MediWerk, the protection of personal data is a top priority. In addition to the GDPR, we also adhere to applicable guidelines and protocols. We are proud of our certification as an occupational health service in accordance with SBCA guidelines and are regularly audited by certifying bodies to ensure this.

Possibility to View and Obtain the Privacy Statement

The privacy statement of MediWerk is available for viewing on the website (https://www.mediwerk.com) and at the head office and branches of MediWerk. The regulation can also be obtained upon request in the form of a copy. This measure ensures that the regulation is easily accessible to all concerned and that they can be aware of how their personal data is processed.

Table of Contents

Feedback and Complaints

We value your feedback and encourage you to contact us if you have any questions, concerns, or complaints about our services or the way we process your personal data. Your input is essential for us to improve our services and ensure we continue to meet our high standards for privacy protection and client care.

The Data Protection Officer (DPO 001830), in this case, J. de Zeeuw, is responsible for overseeing the application and compliance with the General Data Protection Regulation (GDPR). A Data Protection Officer is an official within an organization who oversees compliance with privacy laws, such as the GDPR. The DPO serves as a contact for the data protection supervisory authority and for individuals concerning questions or complaints about the processing of personal data. The DPO ensures that complaints regarding the processing of personal data are taken seriously and that appropriate measures are taken to resolve any issues. The DPO is always reachable by phone at 088-0117500 or via email at fg@mediwerk.com.

MediWerk also wishes to inform you that you have the option to file a complaint with the national supervisory authority, the Dutch Data Protection Authority. This can be done via the following link: https://autoriteitpersoonsgegevens.nl/en/contact-dutch-dpa/contact-us

Data Controller and Contact Information

The data controller for the personal data, as described in this privacy statement, is MediWerk B.V. If you have any questions, comments, or complaints about data protection, please do not hesitate to contact us.

MediWerk B.V.
via post: Siriusdreef 3, 2132WT Hoofddorp
via e-mail: governance@mediwerk.com / support@mediwerk.com
via phone: 088-0117500

Location Den Helder	**Location Hoofddorp**	**Location Schiedam**
Luchthavenweg 6F	Siriusdreef 3	Jan van Galenstraat 62
1786P PP Den Helder	2132 WT Hoofddorp	3115 JG Schiedam

General Definitions

In this regulation, the following terms are defined as:

- **Personal Data:** Any information that can identify you as an individual, directly or indirectly. Examples include your name, email address, physical address, telephone number, as well as digital identifiers such as IP addresses or device IDs. It can also include information about your health, preferences, or behaviours when this information can identify you as a person.
- **Special Category Data:** Categories of personal data that are particularly sensitive by nature and therefore enjoy additional protection. This includes data about your health, race, political opinions, religious or philosophical beliefs, sex life, genetic and biometric data. The processing of these data is strictly regulated and often requires explicit consent.
- **Processing:** Any operation or set of operations performed on personal data, whether or not by automated means. This includes activities such as collecting, recording, organizing, structuring, storing, adapting, retrieving, using, disclosing by transmission, disseminating, and even erasing or destroying data.
- **Registration:** Refers to the system or process by which personal data are collected, stored, organized, and managed. Registration can be digital (e.g., in a database) or physical (in a paper file). Within the context of MediWerk, registration encompasses all activities necessary to systematically collect and manage personal data for the delivery of their services, such as health assessments or disability support. The purpose of registration is to provide a structured overview of the collected personal data, so they can be efficiently used, protected, and if necessary, shared according to applicable privacy laws and with respect for the rights of the individuals concerned.
- **Data Controller:** The entity (natural person, company, or organization) that determines why and how personal data are processed. In the context of MediWerk, they are the data controller because they make decisions about the processing of your personal data within their service provision.
- **Processor:** An external party that processes personal data on behalf of the data controller. Processors perform specific tasks, such as data storage, IT support, or payroll administration, under the direction of MediWerk. They must ensure the security and confidentiality of the data according to the agreed terms.
- **Data Subject:** You, the natural person whose personal data are collected and processed. As a data subject, you have certain rights regarding your personal data, such as the right to access, correct, and delete.
- **Third Party:** An individual or organization that is neither the data subject, the data controller, nor the processor, and who is authorized to process the personal data. This can be a partner organization to which MediWerk shares certain data for specific purposes, such as a laboratory for medical analyses.
- **Recipient:** A natural or legal person, public authority, agency, or another entity to whom personal data are disclosed, whether a third party or not. This means any entity that receives personal data from MediWerk, such as healthcare providers or the government, is considered a recipient.
- **Consent of the Data Subject:** Your free, specific, informed, and unambiguous agreement to the processing of personal data collected about you. This means you must actively agree to the processing, and you must be able to withdraw this consent at any time.

- **Data Protection Officer (DPO):** The DPO is an independent expert in data protection within MediWerk, responsible for overseeing compliance with the GDPR and other privacy laws. This role includes advising the organization, conducting impact assessments, and serving as a contact point for both individuals and the data protection supervisory authority regarding privacy issues. The DPO operates autonomously, without influence, focusing on promoting a culture of data protection and safeguarding the privacy rights of the individuals concerned.

Specific Definitions

In this regulation, the following terms are defined as:

- **Information Systems:** These are digital platforms, databases, and applications used by MediWerk to collect, process, store, and analyse personal data. These systems enable us to efficiently deliver services, support decisions, and fulfil our legal obligations regarding data protection. Information systems are essential for managing client information, employee data, and other vital business processes. We ensure the security of these systems by implementing advanced technical and organizational measures, such as encryption, access control, and regular security audits, to protect the integrity, availability, and confidentiality of the collected personal data.
- **Physician:** A medically qualified professional, such as examination physicians and occupational health physicians, involved in assessing, advising, and guiding individuals in relation to their work capacity, health, and well-being at work. These physicians play a crucial role in conducting medical examinations, developing reintegration plans, and providing medical advice, strictly adhering to professional standards and privacy laws. They have access to certain personal data necessary for performing their tasks, under strict conditions that ensure the confidentiality and security of these data.
- **Absence and Reintegration Teams:** A diverse group of professionals working together to support absence management and the employee reintegration process. Besides examination physicians and occupational health physicians providing medical assessments and advice, these teams also include support staff such as medical assistants, reintegration coaches, and other specialists. Their joint goal is to provide optimal guidance and support to individuals returning to work, taking into account medical, psychological, and work-related aspects. These teams work closely together and share relevant personal data, strictly within the frameworks of privacy legislation and professional confidentiality, to develop and implement effective reintegration plans.
- **Employer:** The organization or person for whom the data subject (employee) performs work and who has a contractual relationship with the employee. In the context of MediWerk's services, such as medical examinations, absence guidance, and reintegration processes, the employer plays a central role. The employer is informed about relevant matters affecting the work capacity and well-being of the employee, within the limits set by privacy legislation. This includes information necessary to support the employee in their reintegration process or manage absence, provided it is in accordance with applicable laws and regulations and respects the privacy of the employee.

- **Employee:** The individual person employed by an employer who uses the services of MediWerk in connection with absence, health assessments, or reintegration processes. The employee is the primary data subject whose personal data are processed by MediWerk with the goal of promoting health in the workplace, supporting the reintegration process, and managing work-related health issues. The protection of the privacy and personal data of the employee is of utmost importance, with all information processed in this context strictly maintained according to applicable privacy legislation and with full transparency to the data subject.

Article 1: Purpose of Data Processing

We are MediWerk, a company that collaborates with employers to provide services in the area of workplace health. We operate in accordance with various laws, including those related to social insurance, medical treatments, healthcare professions, and working conditions. This means that we process personal data in accordance with these laws. MediWerk is responsible for processing these data.

Our purpose in processing personal data is to assist our clients in various areas, including:

- Performing legal tasks that apply to us as specified in the Working Conditions Act, the Improvement of Gatekeeper Act, and the procedure for the first and second year of illness.
- Occupational health care and support of employees at companies and institutions we collaborate with for reintegration and guidance during sick leave, prevention of health problems, and improvement of working conditions.
- Offering and conducting integrated health management, health examinations, and medical screenings.

Article 2: Types of Personal Data Collected by MediWerk

At MediWerk, we only collect the absolutely necessary personal data required for delivering our products and services, as described in Article 1 of our regulations. These include:

- Identification and communication data: This includes name, address, telephone number, email address, and date of birth, so we can effectively communicate with the individuals concerned and provide them with appropriate support.
- Data for workplace and health assessments: This includes medical history, results of health examinations (such as blood pressure, cholesterol levels, BMI), medical imaging, and work-related risk factors (such as exposure to chemicals, noise, ergonomic factors), so we can ensure a safe and healthy work environment.
- Data for reporting to individuals and employers: This includes summaries of health status and examination results, recommendations for work-related adjustments or interventions, evaluations of the overall health condition and any medical limitations, so we can provide transparency about the health situation.
- Guidance data for employees under treatment: This includes treatment plans, progress reports from rehabilitation programs, communication with other healthcare providers or therapists, so we can properly guide employees who are under treatment.
- (Occupational) medical record keeping: This includes medical history, medication history, allergies and intolerances, immunization history, family medical history, so we can have a complete picture of the health situation of the individuals concerned.

MediWerk applies the principle of data minimization by only collecting the personal data strictly necessary for the aforementioned purposes. This helps protect the privacy of the individuals concerned and reduces the risk of unlawful data processing.

Article 3: Legal Basis for Data Processing at MediWerk

MediWerk processes personal data when:

- The data subject has given explicit consent.
- It is necessary to comply with our legal obligations.
- It is necessary to protect the vital interests of the data subject.
- It is necessary to perform a contract we have with a company or to take steps before entering into a contract.
- It is necessary for the legitimate interests of MediWerk or a third party, unless the interests or fundamental rights of the data subject, especially the right to privacy, outweigh it.

3.1. General Conditions for Processing

At MediWerk, we ensure that personal data are processed carefully according to the law. Only individuals bound by confidentiality may process these data, and this is done exclusively for the purposes described in Article 1 of our regulations. We treat personal data confidentially, unless the law prescribes otherwise. In some cases, a final judicial decision may also form an exception to this confidentiality.

3.2. Processing of Special Category Data

MediWerk only processes special category data when it is strictly necessary, such as for the treatment or guidance of the data subject, when written consent has been given, if the data subject has made the data public themselves, for legitimate legal actions, or when there is a substantial public interest. In cases of sick leave and reintegration, MediWerk follows the guidelines (in Dutch) for recording such special category data:

- Richtlijn omgaan met medische gegevens (herziening KNMG, 2024)
- Leidraad bedrijfsgeneeskundig dossier- Inrichting & Overdracht (NVAB, 2021)
- Leidraad Casemanagement bij ziekteverzuimbegeleiding (herziening NVAB, 2020)
- Leidraad Bedrijfsarts en Privacy (herziening NVAB, Oval 2019}
- De zieke werknemer: beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers (Autoriteit Persoonsgegevens, 2016)

3.5. Scientific Research or Statistics

Personal data can be processed for scientific research or statistics if specific conditions are met, such as public interest, privacy protection, and compliance with the WGBO. If obtaining explicit consent is difficult or impractical, other safeguards must be in place to protect the personal privacy of the individuals concerned.

3.6. Use of Identification Numbers

Identification numbers are unique codes used to identify individuals, such as a social security number or passport number. These numbers are only used as prescribed by law, for example, for government services or tax purposes. The purpose is to protect people's privacy and ensure that their personal data are not unnecessarily exposed.

3.8. Automated Decision-Making

At MediWerk, we currently do not use systems that make decisions automatically with a significant impact on you without human intervention. Should we decide to use such technologies in the future, we will communicate this clearly. You will be provided with an explanation of how it works, the reasons for its use, and what it means for you. Importantly, you always have the right to object to such an automatic decision. You can request a review by a person, express your own viewpoint, and challenge the decision. For us, your opinion and privacy always come first.

Article 4: Retention Periods

4.1. Duration of the Retention Period

At MediWerk, personal data are not kept longer than necessary for the intended purpose, unless otherwise prescribed by law or regulation. This means, for example, that employee medical records are retained for the duration of their employment and for the legally required period after the termination of employment, as prescribed by the Occupational Health and Safety Act and other relevant legislation. After this period, the data are securely destroyed to ensure the privacy of the individuals concerned and to comply with legal requirements.

4.2. Application of Retention Periods

The retention periods used are in line with applicable laws and regulations. If desired, these can be requested. This takes into account the type of personal data and the purpose of the processing.

4.3. Deletion and Destruction of Data

Once the retention period has expired, personal data are deleted and destroyed within a reasonable period of up to one year. This is done in a secure and responsible manner to protect the privacy of the individuals concerned.

4.4. Right to be Forgotten

Under certain circumstances, individuals have the right to request the deletion of their personal data. MediWerk will review such requests and, if the legal requirements are met, remove the data. Read more about this in Article 6 of our regulations.

4.5. Periodic Evaluation

MediWerk regularly assesses whether it is necessary to retain personal data and adjusts the retention periods as necessary to continue to comply with changing laws and regulations, as well as the needs of the company.

Article 5: Access to the Registration

5.1. Access Management

Access to personal data is carefully managed according to the 'need-to-know' principle, meaning only employees who need access to certain data for their work actually get that access. This means access rights are assigned based on an employee's role, ensuring only relevant data are accessible to the right people. These access rights are managed through roles, maintaining a clear separation of duties and responsibilities within the organization. For special categories of personal data, such as medical information subject to professional confidentiality, access is limited to the treatment team, providing extra security for sensitive information.

5.2. Management of Access Rights

The granting and modification of access rights follow a standardized procedure. All changes in authorizations are approved by the respective supervisor(s). Functional administrators, along with the IT department, regularly perform checks to identify and resolve conflicting authorizations. In case of any conflicts, the issue is reviewed by the Data Protection Officer.

5.3. Termination of Access Rights Upon Departure

Upon the departure of permanent or contracted employees, the HR department coordinates the termination of all access rights. This includes not just access to the personnel system but also to all other applications and facilities for which the employee had authorization. The implementation of revoking these access rights is managed by the IT department and functional administrators, to ensure all access is withdrawn timely and securely.

5.4. Review of Files for Quality Purposes

Senior professionals may have access to files for quality purposes, within their area of expertise or for supervision over other professionals. This aids in providing the best treatment and guidance to the individual concerned. The findings of the senior professionals are shared with the individual's therapist or guide.

5.5. Access for Maintenance Workers of Information Systems

Only employees designated by MediWerk, such as functional administrators and the IT department, have access to the information systems. This access is solely intended for the maintenance and management of the information systems, such as performing updates, resolving technical issues, and ensuring the overall proper functioning of the systems.

Article 6: Disclosure of Personal Data

6.1. To MediWerk Employees

Personal data are provided to MediWerk employees who are directly involved in the current services and guidance of the individual concerned. This includes treating physicians, case managers, and other professionals involved in the individual's care process. All MediWerk employees are bound by a confidentiality obligation regarding the personal data they encounter in the performance of their duties. This confidentiality obligation is essential to ensure the confidentiality and privacy of the individuals concerned.

6.2. To Data Processors

Personal data are provided to data processors working on the assignment given by MediWerk. These processors include administrative service providers, such as accounting service providers, medical service providers, such as laboratories and medical research institutes, and IT service providers involved in the management and maintenance of information systems. These processors are required to provide adequate safeguards for the protection of personal data according to all provisions of MediWerk's privacy statement.

Before providing personal data to external processors, such as administrative, medical, and IT service providers, MediWerk requires these processors to sign a confidentiality declaration or enter into a processing agreement. A processing agreement is a legal document containing specific provisions regarding the protection of personal data and the responsibilities of the processor according to

applicable laws and regulations and the provisions of MediWerk's privacy statement. These measures are intended to ensure the confidentiality and integrity of personal data and to comply with the requirements of the General Data Protection Regulation (GDPR) and other applicable privacy laws.

6.3. To the Employer

In the case of absence guidance, personal data are provided to the employer. This involves essential information such as the date of the last consultation, limitations, capabilities, reintegration proposals, conclusions on the degree of disability, prognoses, and other process guidance agreements and advice.

6.4. To Reintegration Companies

Reintegration companies receive necessary data for reintegration purposes, even without authorization based on legal regulations. These data include information essential for the reintegration process of employees who have become incapacitated for work and need support to return to work. It may involve details about the health condition of the employee, limitations, capabilities, reintegration proposals, prognoses, and other relevant information required to create and implement effective reintegration plans. Reintegration companies work closely with employers, occupational health services, and other relevant parties to facilitate a structured reintegration process and help the employee resume activities in an appropriate manner.

6.5. To Social Insurance Execution Institutes

Personal data are provided to social insurance execution institutes, such as UWV (Employee Insurance Agency), a Dutch government organization responsible for implementing employee insurances such as WW (Unemployment Insurance Act), WIA (Work and Income according to Labor Capacity Act), and Sickness Benefits Act. Data exchange with UWV occurs in accordance with the individual's reintegration plan, crucial for processes related to incapacity for work, unemployment benefits, and support in reintegration into the labour process. This may involve data related to the employee's incapacity for work, reintegration efforts, and progress reports. This provision of data takes place according to strict guidelines and procedures established by UWV and other relevant regulatory bodies, to ensure careful and targeted support for employees during their reintegration process. By collaborating with UWV, our organization can effectively contribute to the recovery and return to work of the employees concerned, fully complying with privacy legislation.

6.6. To Insurance Companies

Insurance companies receive personal data from MediWerk to facilitate the insurance of wage payment during employee illness. This data exchange follows the provisions of the covenant data exchange between occupational health services and insurers. This may involve information about sickness absence, medical diagnoses, reintegration efforts, and other relevant data required for managing work-related insurance policies. These data are shared in accordance with applicable laws and regulations and the agreements set out in the covenant between MediWerk and the respective insurers.

The data exchange between MediWerk and insurance companies, as described above, is regulated by a specific covenant data exchange between occupational health services and insurers. This covenant is a formal agreement establishing procedures, scope, and security measures for sharing personal data, meeting both the needs of the insurance process and the strict requirements of privacy legislation. The purpose of this covenant is to create a clear framework within which information about sickness absence, medical diagnoses, and reintegration efforts is shared safely and responsibly, supporting the insurance of wage payment during employee illness. This ensures both the privacy of employees and the interests of employers and insurers are protected. By participating in this covenant, MediWerk commits to limiting data exchange with insurers to what is strictly necessary for managing work-related insurance policies and to always ensure the security and confidentiality of personal data.

6.7. To the Minister of Social Affairs and Employment

The Minister of Social Affairs and Employment receives statistical data related to the execution of the tasks of the Data Controller, such as MediWerk. These data may include information about disability rates, absence percentages, reintegration trajectories, and other relevant data related to working conditions and social security. These statistical data are provided at an aggregated level and are used for policy purposes, monitoring trends, and evaluating the effectiveness of social policy in the field of labour market and employment.

6.8. To the Netherlands Centre for Occupational Diseases

The Netherlands Centre for Occupational Diseases (NCvB) receives data in the context of legally required notifications of occupational diseases. This includes information about cases of work-related health problems classified as occupational diseases, as established by the Occupational Diseases Act. Employers and occupational health services are legally required to report certain occupational diseases to NCvB, allowing data to be collected, analysed, and reported on the frequency and nature of these diseases. These data are used for epidemiological research, policymaking in the field of occupational health and safety, and taking preventive measures to reduce the risks of occupational diseases.

6.9. International Data Transfer

In exceptional cases where it is necessary to transfer personal data to countries outside the European Union (EU) and the European Economic Area (EEA), MediWerk takes strict measures to protect your privacy and the security of your data. Such transfers take place based on adequacy decisions by the European Commission, or, if necessary, by using standard contractual clauses or other suitable safeguards that ensure the security of your data. MediWerk aims for complete transparency in these processes and will inform you about the specific measures taken to ensure the security of your data when transferred to third countries.

Your Rights

Right to Information

The right to information means that MediWerk informs you about how your personal data is processed. This is done before the data is obtained, unless you are already aware of this. This information includes, among other things, the purpose of data processing, the categories of personal data that are processed, the legal basis for processing, and to whom the data is disclosed. If necessary, additional information will be provided to ensure you have a clear understanding of the processing of your personal data.

Right to Confidentiality

You can trust that your privacy will be respected at all times. Both MediWerk and all persons working for them are obligated to strict confidentiality regarding the personal data they process. This means that your data is handled securely and only used for the purposes for which it was collected. This obligation to confidentiality remains undiminished unless a legal provision obliges them to disclose certain information. All persons working for MediWerk, such as treating physicians, case managers, and other professionals, are expressly obligated to confidentiality regarding the personal data they have access to. You can therefore trust that your data is in safe hands and that your privacy is protected at all times.

Right of Access

You have the right to know which personal data about you is being processed. This means you can request access to your data at any time. We will handle and respond to your request as quickly as possible, but no later than within four weeks. If desired, we can also provide you with copies of your personal data. However, there may be cases where we must refuse your request for access, for example, if this is necessary to protect the privacy of others or because we suspect that your request for access is made with the intention of abusing your rights or causing harm to our company or other involved parties. We will always inform you if your request for access cannot be granted and explain the reasons. Your privacy and the secure handling of your data are always our top priority.

To ensure that the access request is made by you, we ask you to send a copy of your identification document with the request. In this copy, please black out your passport photo, the machine-readable zone (the strip of numbers at the bottom of the passport), passport number, and Citizen Service Number (BSN). This is to protect your privacy.

Right to Rectification, Suppression, Data Portability, and Objection

You have the right to request correction or supplementation of your personal data if it is factually incorrect, incomplete, or irrelevant to the purpose of processing. When you submit a request for correction or supplementation, we will respond in writing within four weeks. You can also make use of the right to data portability, where you can receive and/or transfer your personal data to another organization. Furthermore, you are free to object to the use of your personal data. Your wishes regarding your data are important to us, and we will treat your requests seriously and carefully.

Right to be Forgotten

You have the right to request in writing the deletion of your personal data. Once we receive your request, we will respond within four weeks and delete your data within three months, unless there is a legal obligation to retain the data or when retention of the data is necessary for another interest. Your privacy is important to us, and we will treat your request with care and attention.

Exercising Your Rights

If you wish to exercise your rights under the General Data Protection Regulation (GDPR), including the right to access, rectify, delete your personal data, or object to the processing of your personal data, you can proceed as follows:

Step 1: Identity Verification

To verify your identity and ensure that we only provide or modify personal data for the lawful owner, we ask you to send a copy of your identification document with the request. In this copy, please black out your passport photo, the machine-readable zone (the strip of numbers at the bottom of the passport), passport number, and Citizen Service Number (BSN). This is to protect your privacy. Additionally, we may ask you additional questions about your date of birth and address details, or send a verification code via email or SMS that you need to confirm.

Step 2: Submitting Your Request

You can submit your request via email, mail, or by filling out an online form available on our website. Please clearly specify which action you want us to take regarding your personal data. Contact information can be found under "Feedback and Complaints" on page 2 of the privacy statement.

Step 3: Processing Your Request

Our Data Protection Officer will register and process your request. We aim to handle your request within the legal term of one month. If we are unable to comply with your request for technical or legal reasons, we will inform you in detail about the reasons.

Step 4: Feedback and Complaints

After processing your request, we will inform you about the actions taken. If you are not satisfied with the handling of your request, you have the right to file a complaint with the Dutch Data Protection Authority.

The Rights of Your Employer

Your employer retains the right to conduct an audit to verify whether MediWerk adheres to the conditions set out in this privacy statement. This audit is carried out by an independent third party engaged by the employer. The purpose of this audit is to ensure that the processing of personal data complies with applicable privacy legislation and that MediWerk adheres to the provisions of this regulation. Through this review, the employer can guarantee compliance with privacy requirements and strengthen the confidence of the individuals concerned in the handling of their personal data.

How We Secure Personal Data

MediWerk strives to prevent personal data from being altered, accessed without authorization, or unlawfully provided to third parties during processing. This includes taking appropriate technical and organizational measures, such as imposing a confidentiality obligation on staff and those involved in executing the processing agreement. These measures are designed to protect personal data against incidents such as destruction, loss, alteration, unauthorized access, and dissemination. They must comply with current standard requirements, as outlined in ISO 27001:2013.

If you believe that your data is not securely protected or there are indications of misuse, please contact our customer service or via governance@mediwerk.com.

Data Processing within the European Union

All personal data is processed within the borders of the European Union, where MediWerk adheres to applicable laws and regulations concerning data protection within this jurisdiction.

ISO 27001:2013 Certification

ISO 27001:2013 is an international standard for information security that provides guidelines for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. Obtaining ISO 27001:2013 certification means that MediWerk meets these standard requirements and has implemented effective security measures to ensure the confidentiality, integrity, and availability of information.

Ongoing Evaluation

Security measures are regularly reviewed and updated to maintain an appropriate level of security, taking into account technological developments and costs. These measures are also aimed at preventing unnecessary collection and processing of personal data while simultaneously providing effective protection against potential risks associated with processing personal data.

Technical Measures

At MediWerk, we take the protection of your personal data very seriously. Therefore, we implement a range of rigorous technical measures to ensure that your data remains secure. By continually investing in advanced security solutions and actively managing risks, we aim to provide a robust and reliable security infrastructure.

Information Systems Management

Our information systems and user systems are continuously and proactively managed. This includes regularly performing patches, updates, and other security-related tasks to address potential vulnerabilities and keep the systems up to date.

Security Measures

We implement security and control measures on user systems. These measures cannot be undone by end-users and are intended to strengthen security. Examples include screen timeouts, session timeouts, the inability to disable security software, and denying administrative rights to end-users on computers.

Security Software

We use security software such as virus scanners and firewalls. These programs detect and prevent malicious software and unauthorized access to our system, thereby protecting your data against cyber threats.

Periodic Penetration Testing

We regularly conduct penetration testing (pen tests) to identify and address vulnerabilities in our systems. These tests simulate realistic attacks on our systems to evaluate security strength and detect any weak points.

Scanning for Technical Vulnerabilities

We actively scan our systems to detect and address technical vulnerabilities. Through automated tools and manual inspections, we regularly check for potential risks and take appropriate actions to improve security.

Applying DKIM, SPF, and DMARC

These are three internet standards we implement to secure your email communication. DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) help prevent email spoofing, phishing attacks, and the sending of malicious software. This reduces the chance of receiving emails containing viruses, spam, or intended to steal your personal (login) information.

Applying TLS (Transport Layer Security)

For sending your data over the internet, we use a secure connection using TLS, formerly known as SSL. You can recognize this by the address bar that starts with 'https' and the lock icon. TLS encrypts data during transmission, preventing it from being intercepted or read by unauthorized parties.

How We Handle Data Breaches

Despite our best efforts to keep your data secure with strong technical and organizational measures, we recognize that no system is infallible. In the rare case of a data breach, where there is a chance that personal data has been lost or processed in a manner that should not be allowed, we will take immediate action.

Our Response to Data Breaches

- **Prompt Action:** If we discover a data breach, we immediately inform both the employer and the individuals concerned, no later than 48 hours after discovering the breach.
- **Assessment and Notification:** We carefully assess whether the data breach must be reported to the Dutch Data Protection Authority and to the individuals concerned, in accordance with the GDPR and the guidelines of the Dutch Data Protection Authority.
- **Responsibility for Notifications:** It is our full responsibility to ensure that notifications to the Dutch Data Protection Authority and to the individuals concerned are done correctly, timely, and completely.
- **Communication:** We keep the individuals concerned and the employer informed of new developments regarding the data breach and the steps we are taking to limit the consequences and prevent it from happening again.
- **Independent Assessment:** As the Data Controller, we will independently decide whether notification of the data breach is necessary to the Dutch Data Protection Authority and to the individuals concerned.

Your safety is our priority

We take your privacy and the security of your data very seriously. In the unfortunate event of a data breach, we will do everything in our power to minimize the impact and communicate transparently about the measures taken.

How We Use Cookies

MediWerk only uses technical, functional cookies, and analytical cookies that do not infringe on your privacy. A cookie is a small text file that is stored on your computer, tablet, or smartphone when you first visit this website. The cookies we use are necessary for the technical operation of the website and your ease of use. They ensure that the website works properly and, for example, remember your preference settings. This also allows us to optimize our website. You can opt out of cookies by setting your internet browser to no longer store cookies. In addition, you can also delete all information previously stored through your browser's settings.