MediCheck

Privacy Policy

The following document was created by Medicheck SA/NV and explains how the organization processes personal data and how it applies data protection principles. It Is available in English, French and Dutch.

1. INTRODUCTION

MEDICHECK S.A./N.V. is a limited liability company organised under the laws of the Kingdom of Belgium. Its headquarters are located at **Place Sainte Gudule 5, 1000 Brussels** and it is registered with the Register of Legal Entities under the number **0683.604.629**. The company is hereby represented by its CEO, **Jean Rifflart** and will be hereinafter referred to as "Medicheck".

A. Purpose of the Privacy Policy

Medicheck is strongly committed to protecting the privacy and security of your personal data. Its mission is to change the codes of medical control and offer a service that is more ethical, positive and constructive for employees as well as more efficient for companies. Ensuring the protection of personal data plays a major role in achieving this goal.

This Privacy Policy was thus established to provide as much transparency as possible to any Data Subject on whom Medicheck processes personal data. It was created in accordance with the European Data Protection Regulation (GDPR) which was adopted on the 14th of April 2016 and which became enforceable on the 25th of May 2018. Medicheck undertakes to adapt this Privacy Policy in the event of any modification made to this Regulation in the future.

Medicheck will also review and adapt this Policy whenever there is a change in its processing activities of personal data. The solution the company offers is a digital one and the evolution and development of its services is perpetual. It thus aims to stay up to date and use the latest technologies and protocols to ensure data security, which implies updating this Policy on a regular basis. **The last update was on the 14/08/2019**. Medicheck's clients and collaborating doctors will be notified directly in the case of any major changes to its processing activities.

B. Scope of the Privacy Policy

This Privacy Policy applies to all personal data processed by Medicheck but focuses mainly on the personal data processed specifically in the context of its medical control activity. To this end, it can be considered as an annex to the main contract governing the relationship between Medicheck and its clients or collaborating doctors. Should there be any discrepancies between the main contract and the Privacy Policy, the latter prevails.

This Policy also allows employees whose personal data is processed by Medicheck whenever they are subject to a medical control to be informed of the processing activities being carried out. This is important given that these workers do not give their direct consent to Medicheck for the processing of their data (see D. Legal basis for the processing for more information).

Finally, a small section of this Policy is dedicated to the personal data that is being processed by Medicheck but not in the context of its medical control activity (for example, if an individual leaves a message about getting some legal advice on the Medicheck website).

C. Key definitions

The following terms and concepts are used throughout this document and are defined here in accordance with the GDPR. Additional information can be found in Article 4 of the GDPR.

"Personal data" is any information that makes a living person identifiable. For example, it includes a person's name, address, phone number, IP address, professional email address, etc.

"Processing" covers all activities relating to the use of personal data by an organisation, from its collection to its storage and disposal and everything in between.

The "data subject" is the person whose personal data is being processed.

"Special categories of personal data" is any data for which a person could be discriminated against (for example a person's race, ethnic origin, religion, health, etc.). These categories of personal data are thus considered to be more at risk and are specifically regulated.

"Data concerning health" are included in the special categories of personal data and are any information related to the physical or mental health status of a person.

The "data controller" is the one with the final say on the purpose and means of the processing of personal data. The controller is both responsible for the processing of personal data as well as ensuring that the personal data is processed in accordance with data protection law.

The "data processor" processes personal data on behalf of the controller. Since the processor does not own the personal data, it only processes this data at the request of the controller.

The "sub-processor" processes personal data under the direct authority of the processor.

The "third party" is anybody, other than the data subject, controller and processor, who is authorised to process personal data under the direct authority of the controller or processor.

The "anonymisation" is the irreversible act of rendering any personal data anonymous in such a manner that the data subject is not or no longer identifiable.

2. PROCESSING IN THE CONTEXT OF MEDICAL CONTROL

This section focuses on the processing of personal data in the context of Medicheck's primary activity of medical control. It details what data Medicheck processes, why and on what legal grounds, but also how Medicheck ensures the security of its processing activities.

A. Context & purpose of the processing

Medicheck is a Belgian company that acts as an intermediary between its client companies and doctors by offering a new medical control solution. When a worker gets sick, the Belgian legislation allows the employer to have an independant doctor reevaluate his or her working incapacity. The employer that wishes to do so goes through organizations like Medicheck to select an independent doctor, schedule the appointment and report its result.

When conducting its services, Medicheck is led to process various personal data on behalf of its client companies and collaborating doctors. **Medicheck thus processes this personal data as a processor under the clients' and collaborating doctors' responsibility**. In this context, **employers and doctors are thus data controllers**.

B. Principles for processing personal data

Medicheck is compliant with the guiding principles described in Article 5 of the GDPR which explain how personal data should always be processed. They are as follows:

(1) **Lawfulness**, **fairness**, and **transparency**: Medicheck respects the law (cf. section D. Legal basis for the processing), only processes personal data in a way that people would reasonably expect and is always open about its data protection practices.

(2) **Purpose limitation**: Medicheck only processes personal data for the specific reason it is collected and for nothing else (cf. section A. Context & purpose of the processing).

(3) **Data minimization**: Medicheck doesn't process more personal data than it needs to (cf. section E. Data minimisation).

(4) **Accuracy**: Medicheck makes sure that any personal data it processes is adequate and accurate (cf. section F. Data quality and accuracy).

(5) **Storage limitation**: Medicheck does not store personal data for longer than it needs to (cf. section G. Retention of Personal Data).

(6) **Integrity and confidentiality**: Medicheck always processes personal data securely (cf. Appendix 1 : Technical and organisational measures for personal data protection).

C. Personal data being processed

Medicheck deals with three data subjects in the context of its medical control activity:

(1) **superiors** that launch the medical controls ;

(2) **workers** on whom the medical controls are performed ;

(3) **doctors** that are tasked by Medicheck to perform the medical controls.

For each data subject, Medicheck processes data among these six categories:

(1) **Standard identification data** (e.g. last and first names, gender, address, function) ;

(2) **Communication data** (e.g. phone number, email address) ;

(3) **Invoicing data** (e.g. bank account number) ;

(4) **Special health data related to an incapacity** (e.g. copy of the medical certificate) ;

(5) **Special health data related to a medical control** (e.g. control location, result);

(6) **Statistical data** (e.g. number of Checks carried out by a doctor)

It is important to note that Medicheck processes data concerning the health of the workers on which controls are performed which are listed in the special categories of personal data of the GDPR and thus require a greater attention as these types of data could create more significant risks to a person's fundamental rights and freedoms. Higher security measures to strengthen the protection of these categories of data are thus considered throughout the entire operational process of medical controls at Medicheck.

D. Legal basis for the processing

The processing of workers' and employers' data to execute medical controls is governed by a contract between Medicheck and its client companies and, similarly, the processing of doctors' data is governed by a contract between Medicheck and its collaborating doctors. These contractual relationships constitute the lawful basis of Medicheck's processing of personal data as specified by Article 6 (1)(b) of the GDPR.

Furthermore, the lawful basis of the processing of worker's health data to operate medical controls is described in Article 9 (2)(b) and (h) of the GDPR. It is considered as necessary for the purposes of carrying out the obligations and exercising specific rights of the controller (the employer or the doctor in Medicheck's case) in the field of employment. It is also necessary for the assessment of the working capacity of the employee.

E. Data minimisation

Medicheck uses data minimization rules at every step of its operational process. The company limits personal data collection, storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out medical controls. For example, more or less data on a worker can be communicated to the doctor depending on the type of control (e.g. the address of the worker will only be communicated to the doctor if the doctor has to perform the control at the worker's home, not if the control occurs at the doctor's office).

F. Data quality and accuracy

Not only is data quality a legal requirement, it is also an operational one for Medicheck. Having an incorrect doctor address for example could imply sending a worker to the wrong location,

making the medical control impossible. The repercussions of such a mistake are not negligible for Medicheck and ensuring the quality of the data being processed is thus a major focus. In this regard, the company benefits greatly from its fully digitized process which guarantees that any data that is inputted by a user of one of its applications (whether in the case of the superior, doctor or back office operator) is entered only once throughout the entire operational process. This removal of redundant inputs minimises the chance of mistakes being made.

G. Retention of Personal Data

Medicheck ensures that the period for which all personal data is stored is limited to a minimum until the purpose for which the data is being processed is fulfilled. The data storage period thus varies depending on the data subject and purpose of processing.

Data subject	Duration of the processing	Justification
Superior personal data	The superior personal data is collected at the beginning of the collaboration with a company and is stored until the end of the collaboration.	The superior data is needed to launch Check requests and is thus stored until they no longer use Medicheck's services.
Doctor personal data	The doctor personal data is collected at the beginning of the collaboration and is stored until the end of the collaboration.	The doctor data is needed to operate any medical Check and is thus stored until Medicheck no longer requires their service.
Check personal data (including the worker's personal data)	The Check related personal data is stored during a period of one year.	The data is stored in case employers have a question regarding a Check after it occured.
	OR stored until the end of the collaboration with the company.	

Once the purpose of the processing is fulfilled, Medicheck anonymizes any personal data. This anonymization is irreversible so that the data subject is no longer and will never be identifiable. The anonymized data is stored by Medicheck for statistical purposes.

H. Sub-Processors

As a processor, Medicheck works with sub-processors to conduct its activity. A list of these sub-processors can be found on our website: https://www.medicheck.io/rgpd.

Medicheck commits to informing its customers and collaborating doctors in writing and in advance of any changes regarding the addition or replacement of any sub-processor. The information will clearly indicate the outsourced processing activities, the identity and contact details of the subsequent sub-processors.

Medicheck's customers and collaborating doctors both have the right to object to the contracting with a sub-processor within a certain time period specified in the contract between the parties. The sub-processors are subject to personal data protection obligations and it is Medicheck's responsibility to ensure that each sub-processor provides sufficient safeguards for the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of the GDPR.

3. DATA RIGHTS

A) General elements

The GDPR grants data subjects several rights over their personal data, including:

(1) The right to be **informed** of any processing made on their personal data ;

(2) The right of **access** to their own personal data being processed ;

(3) The right to **rectification** of incorrect personal data being processed ;

(4) The right to erasure (known as "the **right to be forgotten**") ;

(5) The right to **restrict processing** to refrain a company from some processing ;

(6) The right to **data portability** ;

(7) The right to **object** to the processing of their personal data.

Depending on the data subject and the role Medicheck plays when processing the personal data (processor or controller), the rights above might not be exercised the same way.

A) Medicheck as a data processor

As explained in section 2.A. Context & purpose of the processing, Medicheck acts as a data processor when conducting its medical control activity and processes data on behalf of its clients or collaborating doctors. Since the latters are the data controls, they own the data and have all the rights cited above regarding their data. Any data controler wanting to exercise their rights may send an email to Medicheck at the following address: **security@medicheck.io**.

However, any data subject that is not responsible for the processing (including workers) will have to contact the controller directly in order to exercise their rights. Any personal data processed by a processor in the context of a contractual relationship with a controller must be necessary for the performance of the contract and not just useful. But, for example, allowing a worker to consult his own personal data is not considered as necessary for the execution of the contract. For that reason, **any request must be addressed directly to the controller**.

Medicheck undertakes to respond to any request from a data controller within a reasonable time (less than one month) and to redirect any request from a worker to the data controller.

B) Medicheck as a data controller

The data subject that wants to exercise any of the rights described above or that is dissatisfied with the way Medicheck uses personal information when it is the data controller (cf. section 3. Other Processing) can contact the team directly by email: **security@medicheck.io**. Medicheck makes every effort to respond to requests as fast as possible and guarantees to respond within one month after the receipt of the request in accordance with the obligations in Article 12 of the GDPR. This period may be extended by two

months if necessary but Medicheck will inform the data subject of the extension within one month after the receipt of the request.

APPENDIX 1

Technical and organisational measures for personal data protection

(1) Medicheck's internal and external employees are made aware of the security of information and personal data in particular.

(2) Medicheck has an inventory of assets that is regularly updated. The rules for the use of these assets are defined and clearly communicated.

(3) Medicheck's premises where the information, data and processing devices are located have secure access.

(4) Medicheck implements regularly updated antivirus and anti-malware measures to prevent any alteration or theft of data using malware.

(5) Medicheck has a process for managing access requests. Employees' access is limited to the information necessary for the performance of their duties. System administrator rights are strictly limited to essential persons.

(6) Medicheck has a password policy.

(7) Medicheck has a Backup policy in place that allows data to be restored if necessary (loss, theft, etc.). Restoration tests are regularly carried out.

(8) Medicheck uses security measures to protect information transfers using secure protocols.

(9) Medicheck ensures that security requirements are guaranteed during the development and maintenance of software and systems.

(10) Medicheck ensures the security of the systems and carries out tests before use.

(11) Medicheck has an incident management procedure documented and communicated to staff and authorized third parties.

(12) Medicheck limits the risk of system failure through good maintenance and redundancy.

We hope you've found this Privacy Policy useful.

If you have any questions regarding data security at Medicheck, don't hesitate to send an email at security@medicheck.io. We'll gladly help you out!