Privacy regulations of SZamen Gezond B.V.

These are the privacy regulations of SZamen Gezond B.V., with its registered office at Laan 1914 43, 3818 EX in Amersfoort, hereinafter referred to as SZamen (www.szamen.nl).

We will do everything in our power to ensure personal data is handled carefully, securely and confidentially. We process privacy-sensitive data in accordance with the conditions set out in the General Data Protection Regulation (GDPR) and guarantee professional independence in accordance with the guidelines of the professional statute for working conditions services.

We believe it is important to be transparent about the way in which we safeguard privacy and handle privacy-sensitive information. That is why we explain in these privacy regulations which data we process and for what purposes.

Scope

These regulations implement the right to transparency in accordance with Article 12 of the General Data Protection Regulation (GDPR). These regulations further implement Articles 13 and 14 of the GDPR. These regulations apply to any fully or partially automated processing operation of personal data by SZamen, as well as the non-automated processing of personal data included in a file or intended to be included therein, by persons employed or working on behalf of SZamen.

Responsibility and confidentiality

All employees of our organisation are bound by a duty of confidentiality with regard to confidential information and/or the processing of personal data, which duty is formally arranged upon commencement of employment. These privacy regulations are known to and have formally been accepted by every employee of our organisation. Every employee is therefore obliged to comply with the established guidelines.

Purpose of processing personal data

Personal data is used for the following purposes, including:

- Carrying out our work, to be regarded as the primary service provision, in the context of which an order has been placed with us;
- Informing you about changes to our services;
- Providing information in the form of targeted contacts and any newsletters;
- The maintenance, including updates and releases, of the systems in which privacy-sensitive information is recorded, whether or not made available by a sub-processor;
- The data and technical management, by a sub-processor;
- The hosting, also by a sub-processor;
- Accounting and financial settlement;
- Carrying out commercial activities.

Basis for data processing

The processing of personal data is only lawful if and insofar as certain conditions are met (in accordance with Article 6 of the GDPR). By agreeing to these privacy regulations, our customer explicitly gives consent for the processing of personal data for the purposes referred to above. If no

explicit consent has been given for the processing of personal data, processing cannot take place, unless this is necessary for the performance of the contract to which the data subject is a party. In addition, we may be subject to a legal obligation to process personal data. The basis for this is Article 6, paragraph 1, under a – d.

If we process data for commercial activities, the basis for this is Article 6, paragraph 1, under f. Before processing data for the purpose of carrying out the application procedure, we will ask for your consent first. The basis for this is Article 6, paragraph 1, under a.

Mandatory personal data and access to personal data

In order to provide our services, we process the following data:

- Customer details
- Personal data
- Health data I
- Health data II
- QMS (Quality Management System) data & records
- Financial and administrative data

The categories of data are further specified in Appendix A to these privacy regulations.

Access to personal data

Within our organisation, we apply the following principles with regard to accessing personal data:

- Employees only have access to personal data to the extent necessary for the proper performance of their duties and are contractually obliged to maintain confidentiality.
- Appendix B provides an overview of access per job role. This is the starting point for granting access within the organisation.
- External parties hired by us or otherwise registered to perform work only have access to personal data to the extent necessary for the proper performance of their duties and are contractually obliged to maintain confidentiality.
- Electronic (medical) personal data is secured in such a way that unauthorised persons cannot gain access to this data.

Authorisation procedure

- The employee or external user requiring access to the digital sickness absence management system based on his or her position (see Appendix B) is authorised by the helpdesk employee at the request of management.
- If a user changes position or leaves the employment of SZamen, the authorisation will be terminated at the request of management, effective immediately.

Security

SZamen has taken the appropriate technical and organisational measures to protect personal data against loss, theft or misuse.

The following organisational measures have been taken:

- Only authorised personnel have access to personal data processed in the context of the processing agreement.
- These employees hold the relevant certificates and/or diplomas.
- References are checked prior to commencement of employment.
- Employees are bound by a non-disclosure agreement and the IT infrastructure guidelines as described in the employee handbook.
- Access to the work floor is secured by a key and alarm code.
- Security procedures are tested, kept up to date and evaluated with regard to their effectiveness, security and applicability (by means of supplier assessments).

The following technical measures have been taken by SZamen:

- All personal data is properly protected and encrypted.
- Access to systems is possible only through 2-step verification (2FA).
- The system is designed in such a way that each user only has access to the data that is strictly necessary for his or her work.
- Endpoint Detection and Response (EDR) software is kept up-to-date and is monitored by the IT supplier Welnet.
- A password policy has been established for employee user accounts.
- Personal data received in paper form will be scanned and subsequently destroyed. A policy has been drawn up for this purpose.
- Personal data and/or related files are exchanged via an encrypted solution (ZIVVER).
- SZamen Gezond B.V. does not use external hard drives and/or USB memory sticks.
- Secure back-ups are made of the documents and e-mail.
- As regards software and/or services used for sickness absence and personnel files supplied by SZamen partners, these organisations are evaluated annually to ensure they still hold a valid ISO27001 certification, among other things (by means of supplier assessments).
- A strict retention period policy is maintained.

Finally, we apply requirements that the consultation room of an occupational physician must meet. These requirements are described in our Quality Management System (QMS) and checked annually.

Retention periods

We do not retain personal data for longer than is necessary for the purpose for which it was provided or as required by law.

After termination of employment with the employer or after termination of the working conditions service agreement, reports/documents/data resulting from the Eligibility for Permanent Incapacity Benefit (Restrictions) Act will be permanently deleted from the employer's sickness absence management system after 2 years, with the exception of pseudonymised data used in sickness absence reports or documentation expected to be retained, such as data pertaining to WIA benefits or employer rehabilitation obligations. Pre-employment medical examination files are retained for a maximum of six months.

Retention period of medical files

The occupational physician retains medical files for a maximum of 20 years, in compliance with the statutory retention period. It is possible that, if the employee's situation so requires, the medical file will be kept for a longer period. In the event of a risk of occupational conditions developing over an (even longer) period of time, medical data for this purpose must be retained for this longer period of time* as well.

*the retention period for the above is 40 years in the event of an employee being exposed to carcinogenic substances or biological agents. In the event an employee has worked with ionising radiation, the data must be retained until the data subject, to whom the data relates, was last exposed at least thirty years ago, or until the employee has reached the age of seventy-five.

Once the retention period has expired, the personal data will be removed from the system and/or destroyed within three months. An exception is possible in situations where it can be expected that retention of personal data is important and necessary in compliance with the statutory guidelines. In that case, the employer will be notified accordingly.

If employee data needs to be deleted because the retention period has (almost) expired, we will receive an overview of this in the sickness absence management system. The helpdesk employee notifies the employer and permanently deletes the data.

Rights

Right of access

The data subject whose personal data we process has the right to access this data without having to give a special reason. We will provide the necessary information in writing, as soon as possible. SZamen may reject excessive requests for information. Requests are considered excessive if the data subject approaches us with requests for information more than average and/or necessary. Finally, we may charge costs for providing personal data, insofar as not excluded in the GDPR.

Right to object and correct

This data subject can also object to the processing of personal data (or part thereof) by us or by one of our processors. In addition, this data subject has the right to have incorrect personal data changed or to have an additional statement provided. We will notify this data subject immediately, once the relevant data has been rectified.

Right to data portability, revocation and deletion

This data subject further has the right to have the data provided transferred by us to himself or herself or to another party, if so requested. An employee retains the option to withdraw consent for the processing of personal data. However, if we are not permitted to process certain data, we may not be able to provide the data subject or party with a proper service.

Finally, this data subject has the right to have his or her personal data destroyed. This request may be refused if a legal provision is required or if continued retention may be of significant importance to a party other than the data subject. In addition, data may be retained in anonymised form after the request.

The data subject whose personal data we process can send a request for access, objection, correction, data transfer, revocation and/or deletion of his or her personal data, or a request for withdrawal of consent or an objection to the processing of his or her personal data to fg@szamen.nl. We may ask for a valid ID before we can comply with any of the aforesaid requests.

Provision of data to third parties

Personal data will only be provided to a third party if this is required by law or if it is provided with the consent of the registered data subject or his or her authorised representative.
In addition, personal data is provided to third parties if this is necessary for the provision of services.

If personal data of one or more data subjects is provided by us, or if personal data must be provided to us, the personal data will be sent via ZIVVER.

We use an e-mail system through which secure e-mailing is guaranteed. The e-mail and attachments can only be opened with a personalised password. The recipient's response is sent back to us in a secure environment. Personal data may be provided to us by an employee (of an employer), an employer, the Employee Insurance Agency (UWV) or the occupational physician.

We will notify the data subject whose personal data we need to share for very specific reasons, or other than discussed, in order to properly perform our services. In that case too, we use ZIVVER. You can read more on the ZIVVER website.

No reports are made to the employer about an employee attending a working conditions consultation or having undergone voluntary periodic examinations. If an employee of an employer has attended a working conditions consultation or undergone a periodic examination and the occupational physician wishes to provide the employer with advice, we will ask the employee for written consent first. This consent is recorded in the medical file.

The employee has the right to have the data provided by us destroyed, see Rights.

Transfer of personal data

Personal data will always be transferred in compliance with legal requirements. We will ask the employee for written consent for this. In addition, data is only transferred in a secure manner, see provision of data to third parties.

Medical data too will be transferred in compliance with the legal requirements. Only the occupational physician and the medical secretariat are authorised to do this.

In addition to the option to share personal data based on the employee's consent, the occupational physician can share personal data based on necessity (for proper diagnosis/treatment, guidance, rehabilitation of a sick employee or to formulate an answer when asked whether an exception to the obligation to continue paying wages applies).

The following data is covered by the necessity requirement:

- Functional limitations and implications thereof for the type of work the employee can still perform;
- The activities that the employee is still capable of, or no longer capable of;
- The expected end goal of the rehabilitation (suitability for own work, suitable employment or second-track rehabilitation) with, if possible, an indication of the expected duration of the limitations or incapacity for work;
- Any adjustments, work arrangements or activities that the employee and employer must make in the context of rehabilitation;

- Work-related causes of incapacity for work, which may result in repeated incapacity or damage to health upon return to one's own work situation. The employer must be enabled to take appropriate measures;
- Advice on technical interventions facilitated by the employer, such as workplace surveys, workplace adjustments or advice on involving an occupational expert or rehabilitation agency.

Complaints

If you are dissatisfied with the way we handle personal data, you can file a complaint. For this we refer to the complaints procedure on our website. We further remind you of the option of filing a complaint with the national supervisory authority, the Dutch Data Protection Authority.

Data breaches

In the event of a data breach, whether or not the breach is subject to a reporting obligation, we follow an internal data breach protocol. In addition, we carry out a DPIA (Data Protection Impact Assessment) with regard to information security at least once every three years.

Contact

We reserve the right to change these privacy regulations. If a definition appears to be invalid, only this definition will be deleted from the regulations. Following an amendment to the privacy regulations, the regulations and the most recent changes will be published on our website.

Our Data Protection Officer is responsible for updating and enforcing the privacy regulations. The management at all times remains ultimately responsible for compliance and supervision.

The formal controller is:
SZamen Gezond B.V.
Laan 1914 43
3818 EX Amersfoort

For questions or comments about the privacy and protection of personal data in our organisation, we refer you to our Data Protection Officer:

E-mail address: fg@szamen.nl
Telephone number: 033-2859242

Appendix A Categories

Customer details

- Name and address details
- Contact persons
- Agreements

Personal data

- Name and address details
- Date of birth
- Telephone number
- E-mail address
- Nationality
- Gender
- Date: Entry and leaving the employment
- Salary details (optional)
- BSN number *
- Position
- Working hours per week
- Sickness absence data **
- Pseudonymised data

*The Citizen Service Number (BSN), which is prescribed by Dutch law to identify a person, is exclusively used when processing personal data for the implementation of the relevant law or for purposes determined by law.

**Data on sick leave and (expected) return-to-work reports, number of sick days, degree of (in)capacity for work.

Health data I

- Employment options and work capacity
- Bottlenecks position and quality of employment relationship
- Limitations and rehabilitation activities
- Biometric data
- Reports to the UWV (non-medical)

Health data II

- Nature and cause of the illness (diagnosis)
- Information about consultations (examination, diagnosis, report)
- Information about current or past health problems
- Data from (family) doctors, medical specialists and other physicians, requested with the consent of the data subject
- Consent Forms for requesting health data/medical information
- Reports to the UWV (medical and non-medical)

QMS (Quality Management System) data & records

- Company policy
- Complaints (registrations)
- Audit data (registrations)
- Measures for improvement

- Procedures and instructions
- Protocols
- Regulations
- Management reviews

Financial and administrative data

- Name of organisation
- Name and address details
- E-mail address for invoice
- Bank account number
- Signature for agreement

Categories of data subjects

- Employees (and their partners, is applicable);
- Suppliers;
- Customers;
- Service providers.

Appendix B Access to personal data

Documentation, Data, Information Management & Labelling

Labelling and management
Documented Data and Information

	Management Board & QA Management	Youth healthcare physician	Company doctor	Medical secretary	Absenteeism consultant	Case manager task delegation	Occupational consultant	Rehabilitation Consultant Track 2	Accounting Assistant	Secretary (Help Desk)	Data Protection Officer	Core expert
Customer details Confidential - high												
Name and address details	M&C	C	C	M&C	M&C	M&C	C	C	C	M&C-M	C	C
Contact persons	M&C	C	C	M&C	M&C	M&C	C	C	C	M&C-M	C	C
Agreements	M&C	C	C	M&C	M&C	M&C	C	C	C	M&C-M	C	C
Personal data Confidential - high												
Name and address details	M&C	C	C	M&C	M&C-M	M&C	C	C	C	M&C	X	X
Health data 1	M&C	M&C	M&C	M&C	M&C-M	M&C	M	M	X	X	X	X
Health data II	M&C	M&C	M&C	M&C-M	X	X	X	X	X	X	X	X
KMS data and registrations Confidential - medium												
Company policy	M&C-M	C	C	C	C	C	C	C	C	C	C	C
Complaints (registrations)	M&C-M	X	X	C	C	C	X	X	C	C	C	X
Audit data (registrations)	M&C-M	C	X	C	C	C	X	X	C	C	C	X
Measures for improvement	M&C-M	C	C	C	C	C	C	C	C	C	C	C
Procedures and instructions	M&C-M	C	C	C	C	C	C	C	C	C	C	C
Protocols	M&C-M	C	C	C	C	C	C	C	C	C	C	C
Regulations	M&C-M	C	C	C	C	C	C	C	C	C	C	C
Management reviews	M&C-M	X	X	C	C	C	C	C	C	C	C	X
Financial and administrative data Confidential - high												
Name and address details	M&C	X	X	X	X	X	X	X	M&C-M	M&C	X	X
Email address (invoicing)	M&C	X	X	X	X	X	X	X	M&C-M	M&C	X	X
Bank account numbers	M&C	X	X	X	X	X	X	X	M&C-M	M&C	X	X

Authorities	
M&C	Mutations & consultation
C	Consultation
M	Management documents & data*
X	No access

- **Management documents & data**

Distribution, usage & findability
Accessibility & storage method
Changes & version control
Archiving & maintenance
Destruction & clean up