PROCESSING AGREEMENT

1. General

In this processing agreement, the following terms are defined as stated below:

1.1 **General Terms and Conditions**: the General Terms and Conditions of the Processor, which are fully applicable to any agreement between the Processor and the Controller and which form an integrated part of this processing agreement.

1.2 **Processor**: SZamen Gezond B.V., listed in the trade register under number 71847790, and with its principal place of business at Laan 1914 43 in Amersfoort.

1.3 **Data**: the personal data as defined in Appendix 1.

1.4 **Client**: the natural person or legal entity who instructs the Processor to perform the Work, i.e. the Controller.

1.5 **Agreement**: any agreement between the Client and the Processor for the performance of Work by the Processor for the Client, in accordance with the provisions of the confirmation of the instruction.

1.6 **Controller**: the Client who, in his capacity of a natural person or legal entity, has instructed the Processor to perform the Work.

1.7 **Work**: all work that has been assigned or which is performed by the Processor for other reasons. The foregoing applies in the broadest sense of the word and, in any event, includes the Work set out in the confirmation of instruction.

2. Applicability of the processing agreement

2.1 This processing agreement applies to all data collected by the Processor for the Client within the framework of the execution of the Agreement with the Client, as well as to all Work arising from the Agreement for the Processor and the data to be gathered within that framework.

2.2 The Controller is responsible for processing the Data about certain categories of data subjects as described in Appendix 1.

2.3 When executing the Agreement, the Processor processes certain personal data for the Controller.

2.4 This is a processing agreement within the meaning of Article 28, paragraph 3 of the General Data Protection Regulation (GDPR), which governs the rights and obligations regarding the processing of personal data in writing, including security. This processing agreement is binding on the Processor with regard to the Controller.

2.5 This processing agreement, as well as the General Terms and Conditions of the Processor, form a part of this Agreement and all future agreements between the parties.

3. Scope of the processing agreement

3.1 By giving the instruction to perform Work, the Controller has instructed the Processor to process the Data on behalf of the Controller, in the manner set out in Appendix 1, in accordance with the provisions of this processing agreement.

3.2 The Processor only processes the Data in accordance with this processing agreement, particularly so in accordance with the provisions of Appendix 1. The Processor confirms not to process the Data for other purposes.

3.3 Control of the Data will never rest with the Processor.

3.4 The Controller can give additional, written instructions to the Processor on account of amendments or changes to the applicable personal data protection regulations.

3.5 The Processor only processes the Data within the European Economic Area.

4. Confidentiality

4.1 The Processor and the persons employed by the Processor or who perform activities for him, insofar as these persons have access to personal data, only process the Data on behalf of the Controller, subject to deviating legal obligations.

4.2 The Processor and the persons employed by the Processor or who perform activities for him, insofar as these persons have access to personal data, are obliged to keep the personal data which they become aware of secret, except insofar as any legal requirement obliges them to disclose the data or the requirement to disclose is dictated by the task.

5. No further provision

5.1 The Processor must refrain from sharing the data with third parties or otherwise making these available to them, unless the Processor has obtained prior written approval or instructions from the Controller to do so, or is otherwise obliged to do so by virtue of mandatory law. If, by virtue of mandatory law, the Processor is obliged to share the Data with third parties or otherwise make it available to them, the Processor must notify the Controller thereof in writing unless this is not permitted.

6. Security measures

6.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The security measures currently taken are set out in Appendix 2.

6.2 The Processor must take measures which are aimed at preventing personal data from being collected and processed unnecessarily, among other things.

6.3 The Data will only be stored and processed within the European Economic Area.

7. Monitoring compliance

7.1 The Processor will provide the Controller at its request and at its expense with information about the Processing of the Data by the Processor or Sub-Processors. The Processor will provide the requested information as soon as possible, but at the latest within five working days.

7.2 The Controller has the right once a year and at its own expense to have an independent third party jointly designated by the Controller and the Processor perform an inspection to verify whether the Processor complies with the obligations under the GDPR and this processing agreement. The Processor will provide all reasonably necessary cooperation. The Processor has the right to charge its costs associated with the inspection to the Controller.

7.3 In the context of its obligation under paragraph 1 of this article, the Processor will in any case provide the Controller or a third party engaged by the latter with:

- 7.3.1 all relevant information and documents;
- 7.3.2 access to all relevant buildings, information systems and Data.

7.4 The Controller and the Processor will consult each other as soon as possible after the report has been prepared to address any risks and shortcomings. The Processor will take measures at the expense of the Controller to bring the identified risks and shortcomings to a level acceptable to the Controller or to remove them, unless the parties have agreed otherwise in writing.

8. Data breach

8.1 As soon as possible after the Processor has learned about an incident or data breach that (partially) relates to or can (partially) relate to the Data, the Processor must notify the Controller thereof using the Controller's contact details held on record at the Processor and the Processor must provide information on the nature of the incident or the data breach, the Data, the confirmed or expected impact the incident or data breach will have on the Data and the measures taken and to be taken by the Processor.

8.2 The Processor will support the Controller in notifying the parties concerned and/or the authorities.

9. Sub-Processors

9.1 If the Processor has prior (general) permission to outsource its obligations to third parties, the Processor will inform the Controller of the intention to engage the sub-processor. The Processor gives the Controller a period of seven working days to object to the engagement of the sub-processor. The Processor will only engage the sub-processor if the period of seven days has expired without the Controller having objected, or if the Controller has indicated that it does not object to engaging the sub-processor.

9.2 If the Processor does not have prior permission to outsource its obligations to third parties, the Processor will request prior permission for engaging the sub-processor.

9.3 The Processor ensures that the sub-processor is subject to this processing agreement or to the contract for services with the processor which contains defined agreements and responsibilities with regard to the processing of personal data and the provisions in accordance with the GDPR.

10. Data subject rights and duties to cooperate

10.1 When asked, the Processor will cooperate with the Controller in the event of a complaint, question or request from a data subject, or investigations or inspections by the Dutch Data Protection Authority.

10.2 The Processor will assist the Controller at its request and expense in carrying out a data protection impact assessment.

10.3 If the Processor receives a request directly from a data subject to inspect, correct or delete his or her Data, the Processor will inform the Controller within two working days of receiving the request. The Processor will carry out all instructions given by the Controller to the Processor in writing as a result of such a request from the data subject as soon as possible. The Processor takes the necessary appropriate technical and organisational measures that are necessary to comply with such instructions from the Controller.

10.4 If instructions from the Controller to the Processor conflict with any statutory provisions regarding data protection, the Processor will report this to the Controller.

11. Term and Termination

11.1 This processing agreement is valid as long as the Processor is under the instruction from the Controller to process Data under the Agreement between the Controller and the Processor. As long as the Processor performs Work for the Controller, this processing agreement applies to this relationship.

11.2 If after the termination of the Agreement, on the basis of a statutory retention obligation, the Processor is obliged to retain certain data and/or documents, computer disks or other data carriers on or in which Data is located for a statutory term, the Processor will ensure the destruction of this data or these documents, computer disk or other data carriers, within four weeks of termination of the statutory retention obligation.

11.3 In the event of termination of the Agreement between the Controller and the Processor, the Controller, within two months of the termination of the Agreement, may request the Processor that all documents, computer disks and other data carriers, on or in which data is located, are returned to the Controller, at the Controller's expense. In the event of return, the Processor will provide the data in the format as held at the Processor. Insofar as the Data is located in a computer system or in another form through which the Data cannot reasonably be provided to the Controller, the Processor will provide the Controller with an accessible, legible copy of the Data. After this period has expired, the Processor will proceed to permanently destroy the Data, unless the Processor is obliged to store Data on the basis of a statutory obligation.

11.4 Without prejudice to the other provisions of this article 12, the Processor must refrain from keeping or using Data after termination of the Agreement.

11.5 The manner of destruction is determined in consultation with the Controller. After destruction, the Processor will provide the Controller with written confirmation of this.

11.6 Without prejudice to the other provisions of this article 12, the Processor must refrain from keeping or using Data after termination of the Agreement.

12. Nullity

12.1 If one or more provisions of this processing agreement are void or voided, the other conditions will remain in full force. If any provision of this processing agreement is invalid, the parties will confer about the contents of a new provision, which provision will reflect the contents of the original provision as closely as possible.

13. Applicable law and choice of forum

13.1 This processing agreement is governed by Dutch law.

13.2 All disputes in connection with the processing agreement or its implementation will be submitted to the competent court of the central Netherlands.

APPENDIX 1 DATA, PURPOSES AND CATEGORIES OF DATA SUBJECTS

DATA

The Controller instructs the Processor to process the following Data within the framework of the instruction, which may include, but is not limited to, absenteeism management, recruitment & selection, individual and team development or personnel administration.

(1) Name
(2) Name and address details of personnel of the Controller
(3) Contact details
(4) Personal details
(5) Financial information, both business and private
(6) Sickness absence data (in connection with WVP)
(7) Career and educational background
(8) Pseudonymised personal data of personnel of the Controller
(9) General information of the Controller that can be traced back to a person
(10) Employment
(11) Signature of Data Subject or Controller
(12) Data of employees (or third parties) of the Controller

PURPOSES

The activities for which the aforesaid Data may be processed, only if necessary, in any case include:

(1) the activities, to be considered as the primary service provision, within which framework the Controller has issued an instruction to the Processor;
(2) the maintenance, including updates and releases of the system made available by the Processor or sub-processor to the Controller;
(3) the data and technical management, including that of a sub-processor;
(4) the hosting, including that of a sub-processor.

DATA SUBJECT CATEGORIES

The Data that is processed concerns the following categories of data subjects:
(1) Employees (and their partners, is applicable);
(2) Suppliers;
(3) Customers;
(4) Service providers.

APPENDIX 2 SECURITY MEASURES

The Processor has at least taken the following security measures:

Measure	Description
IT Zeker service Workstations	Asset Tracking Patch Management ID Management Managed Antivirus SLA Control Agent Password Manager
Backup and Disaster Recovery	SaaS 365 Endpoint Backup (Email/Sharepoint and OneDrive documents) Backup Azure Blob Storage and Database
Antispam & Antivirus	Antispam & Antivirus protection for email traffic URL and Attachment Defence
Password policy	• Change password every 90 days • Password contains a minimum of 8 characters • Complexity enabled • Previous passwords not remembered 3x • Lock account after wrong password 5x
Group rights	File and Share Rights at Group Level
2-Factor Authentication	2-Step Authentication for local workstation and Azure login
CMDB Database	Asset registration Contacts of the organisation SSL Certificates Documentation Password vault
Encryption	BITLocker Encryption local workstations SSL encryption Space2Work portal ZIVVER communication encryption Password vault AES-256bit and unique AES key per password