Workload Analyser
measure your work pleasure!

Data processing agreement

General description
The data processor shall deliver to the data controller the services agreed with regard to the Workload Analyser as set out below. In this context, the data processor shall process all personal data for and on behalf of the data controller as referred to in the General Data Protection Regulation (in Dutch the Algemene Verordening Gegevensbescherming or "AVG") and set out below, to which the data controller is entitled (hereinafter “personal data”). The data processor is not allowed to process the personal data for its own purposes and/or to divulge these data to third parties.

About the Workload Analyser
The Workload Analyser was developed for employees, managers and health & safety coordinators of insurance companies at the request of the Dutch Association of Insurers. The purpose of the Workload Analyser is to put the topic of workload on the agenda in a constructive manner, enabling employees and employers to take an active and positive approach to conversations regarding workload and work pleasure, and to take action where necessary.

All insurance companies in the Netherlands may make use of this tool. A contact person requests a licence code online on behalf of the organisation. This contact person becomes the coordinator for the company. The licence code gives the coordinator access to the dashboard. By accepting the licence code, the coordinator automatically accepts the terms of this data processing agreement for the Workload Analyser.

Companies that decide to use the Workload Analyser are themselves responsible for entering the data needed in order to use the Workload Analyser in their organisation. This means the participating insurance company is the data controller with regard to the personal data processed in the Workload Analyser. The data processor is Markant IT, located in the Dutch town of Vreeland.

Which data are processed?
With regard to participants using the Workload Analyser, the following data are processed:

- First and last name
- E-mail address

It goes without saying that all personal data are treated with due care. The data processed in the Workload Analyser are combined and processed anonymously. The employee's personal data are **not** linked to the results. In other words, there is no connection between the employee and his/her answers: anonymity is guaranteed.

Retention of the data
Personal data are not kept longer than is strictly necessary in order to achieve the purposes for which they have been collected. The data processor shall observe the following retention periods:

Description	Retention period
First and last name of the coordinator	1 year*
E-mail address of the coordinator	1 year*
First name of the manager (after the invitation from the coordinator)	4 weeks
First name of the manager (after registration by the manager)	6 months*
E-mail address of the manager (after the invitation from the coordinator)	4 weeks
E-mail address of the manager (after registration by the manager)	6 months*
First name of the employee	4 weeks
E-mail address of the employee	4 weeks

* The coordinator and the supervisor receive 4 weeks before the end of the term an e-mail, containing the option to extend it for the same period.

Duty of confidentiality
All individuals employed by or working for the data processor are under a duty of confidentiality.

Security
The data processor shall take technical and organisational measures with regard to the processing of personal data in order to prevent loss or unlawful processing (such as unauthorised access, damage, modification or disclosure of the data).
This includes but is not limited to the following measures:

- pseudonomisation and encryption of personal data;
- security and privacy enhancing technologies.

The data processor shall ensure that staff authorised to process the personal data are bound by a duty of confidentiality during and after their employment (for example by signing a non-disclosure agreement), to the extent that they are not already required by law to observe confidentiality.

The data processor acknowledges that these technical and organisational measures may change in due course and that effective security measures require regular evaluation and improvement. The data processor shall therefore regularly evaluate, tighten and/or improve these measures in order to comply and stay compliant with the requirements and obligations mentioned above.

Other obligations
If a data subject submits a request under his/her legal rights within the meaning of the GPDR (in Dutch: AVG), the data controller shall address the request. The data processor shall cooperate in this process. The data processor shall also help the data controller fulfil other obligations, such as report data leaks, carry out data protection impact assessments (DPIA) and conduct prior consultations.

Reporting data leaks
The data processor shall report any data leak to the data controller within 24 hours, providing information on the nature and scope of the data leak and the measures taken in response to the data leak.

Sub-processors
The Workload Analyser used by NN is hosted by TransIP B.V., located at Vondellaan 47, 2332 AA in Leiden, and registered at the Chamber of Commerce under number 24345899. The personal data are saved in a server in the Netherlands.

The data processor shall not engage any other sub-processor without prior written permission of the data controller. The data processor shall conclude a sub-processor agreement with the sub-processor under which the sub-processor is also bound to the obligations that the data processor has towards the data controller.

Accountability

1. The data processor shall provide the data controller with the information needed by the data controller to assess the data processor's compliance with this agreement.
2. The data processor shall provide the data controller, at its first request, with an explanation of the design and details of its measures and procedures aimed at complying with this agreement.
3. With regard to the processing of personal data, the data controller shall be entitled to inspect the technical and organisational security measures taken by the data processor during the term of this agreement. In this respect, the data controller shall be entitled to request the data processor to submit all relevant reports regarding IT security or privacy audits. In addition, the data controller shall be entitled to conduct audits regarding the processing of personal data by the data processor. The data processor shall provide the data controller with all information needed to conduct these audits.

Upon request, the data controller may conduct (or commission) a security audit with regard to the relevant generic infrastructure, customer specific infrastructure and the information security policy of the data processor by qualified employees and/or third parties.

Audits of the infrastructure and systems used for multiple customers are permitted, provided the interests of these customers are not harmed. This is to be determined by the data processor in advance.

The data processor and its sub-processor shall provide the auditors acting on behalf of the data controller with all reasonable cooperation regarding the audit and with access to the facilities at which the personal data are processed.

Use of cookies

The Workload Analyser only uses functional cookies needed to operate the tool.

Liability

1. If the data processor causes any loss or damage as a direct consequence of non-compliance with this agreement or legal regulations and/or requirements regarding the protection of personal data, the data processor shall be held liable for such loss or damage.
2. The data processor shall never be held liable for any loss or damage caused by the data controller's non-compliance with this agreement or legal regulations and/or requirements regarding the protection of personal data.