DATA PROCESSOR AGREEMENT

1 Parties

Data Processor: Benelizer A/S, Slotsmarken 18, 2970 Hørsholm, Denmark.
Business registration (CVR) 37 36 77 37 (Benelizer)

Data Controller / Data Manager:
Any subscriber to the Benelizer application (Customer)

2 Agreement, Main agreement and Privacy Policy

The ”Data Processor Agreement” (Agreement) regulates the processing of personal data on behalf of the customer (the ”Data Controller”). It is an Addendum to the Benelizer Standard Terms and Conditions for subscription to the Benelizer application (Main Agreement). Benelizer maintains the underlying IT infrastructure and software according to the Main Agreement. The Agreement is complemented by Benelizer Privacy Policy. The Agreement and Benelizer Privacy Policy is published at Benelizer’s website.

In case of discrepancy between the Data Processor Agreement and the Main Agreement or the Privacy Policy it is the Data Processor Agreement that takes priority.

The “Governing law and venue” for the Main agreement shall also apply for any disputes regarding the ”Data Processor Agreement”.

3 Benelizer employees and partners

Benelizer's employees and partners are subject to confidentiality in the treatment of personal data and are also instructed to comply with Benelizer’s Privacy Policy and Data Processor Agreements.

4 Legislation

The Agreement shall ensure that the parties comply with the applicable data protection and privacy legislation, including The European Parliament and the Council’s Regulation 2016/679 of 27 April 2016 on the protection of persons with regard to the processing of personal data applicable on 25 May 2018 (GDPR).

Benelizer will cooperate with supervisory authorities whenever required.

5 Data processing, disclosure and location

See Appendix 2 regarding the nature of the personal data processed under this Agreement.

Benelizer is authorized to process personal data on the Customer’s behalf, according to the terms set forth in this Agreement.

All persons working for or on behalf of Benelizer are instructed to process the Customer’s personal information only after instructions from the Customer.

When relevant Benelizer will make prior consultation and assist the Customer to assess impacts concerning the data processing.
Data is stored at servers in Denmark – including back-up copies.

Benelizer and sub-contractors may not store, process, or in any way make accessible any data outside EU/EØS in unsecure 3rd countries.

6 Technical and organizational safety measures

Benelizer has assessed the risks involved in the processing of personal data by the Customer and have taken appropriate technical and organisational measures to ensure a level of security that prevent information from being accidentally or illegally destroyed, lost or impaired, and against come to the knowledge of the unauthorized person, abused or otherwise treated in violation of the law on treatment of personal data.

Benelizer shall, at the Customer's request, provide the Customer with sufficient information to ensure that the technical and organizational measures have been taken.

Benelizer will on an ongoing basis ensure that servers and other technical equipment are updated and maintained in order to prevent unauthorized access and in order to ensure that authorized access is restored as quickly as possible after any technical faults or physical impacts rendering data inaccessible.

Further details are described in Appendix 1.

7 Documentation for compliance with obligations

Benelizer's hosting sub-contractor (paragraph 15) will from January 2019 annually request an independent accountant to compile an ISAE 3000 periodic declaration regarding compliance with the hosting sub-contractor's obligations related to GDPR. The Customer can request a copy of this declaration.

The Customer can - if it is necessary - choose to initiate and participate in a compliance inspection/audit at the sub-contractor. Such a request must be given with reasonable notice and the Customer must carry the cost for time spent – at a reasonable cost - by the sub-contractor during the inspection/audit.

8 Notification duty

Benelizer informs the Customer without unnecessary delay in case of deviations from agreed delivery.

9 Customer's Instructions to Benelizer

The Customer determines for what purposes and how to process personal data.

Benelizer may not, without written agreement, disclose any data to any third parties or authorities, except as part of Benelizer's compliance with EU law or national law of the EU Member States. In such case, Benelizer shall immediately notify the Customer, unless prohibited by the legislation.

10 Data processing outside of instructions

The data processor can process personal information outside of instructions, only in cases where authorities In accordance with Danish law require this.

11 Customer's responsibility

Personal data in the Benelizer application is the responsibility of the Customer.
The Benelizer application is intended to record general personal data for users such as name, e-mail, telephone number and log of activity.
Customers should not register and type in any sensitive personal data in the Benelizer application including comments fields made available for entering free text. Sensitive personal data include information about race, ethnic origin, religion or philosophical beliefs, sexual orientation, health, political preferences and worker's union membership.

12 Administrative Access for Benelizer

Benelizer ensures that the persons authorized to process personal Customer data are instructed to treat personal data confidentially.

13 Access

It is solely operating staff of Benelizer (and sub-contractor), who has physical and logical access to the IT environment, in connection with ensuring the performance, capacity and ongoing backup.

14 Handling of data after termination of the subscription agreement

Benelizer will after request from the Customer by best efforts, and at the expense of the Customer, extract and deliver the Customer's data in a machine readable format.
Benelizer is required to delete the Customer's data, including personal data, after request from the Customer unless there is a legal requirement to store the information.

15 Sub-contractor (sub-processor)

Benelizer is given general authorization to engage a third-party to process the Personal Data.
The sub-contractor is: Netgroup A/S, Store Kongensgade 40H, 1264 Copenhagen K.

Benelizer remains liable for not breaching the Agreement even if the sub-contractor fails to comply.

In case Benelizer wishes to replace the sub-contractor or include another sub-contractor, the Customer shall be informed and must agree in writing to the changes. If the Customer cannot accept the changes, the Customer can terminate the Agreement – including the Main agreement.

Benelizer and Netgroup has entered a written back-to-back agreement that ensures the terms and conditions for the Data Processer Agreement with the Customer also applies to Netgroup wherever relevant. The Customer can request a copy of this agreement. It is the responsibility of Benelizer to monitor and ensure that the sub-contractor comply with the back-to-back agreement.

16 Security breach

Benelizer assists the Customer as necessary and reasonable in connection with security breaches. In case of a security breach at Benelizer which can compromise personal data, the Customer shall be informed without unnecessary delay. The information must include the nature of the security breach that occurred, the categories of persons at risk and the number of personal data at risk. It will also include information on the measures taken by Benelizer to mitigate the incident. Benelizer is required to investigate the circumstances at his own expense.

17 Breach of the Agreement and liability

The Main Agreement's regulation of breach of contract and the consequences hereof shall apply equally to this Agreement as an addendum to the Main Agreement, including the terms for each party's cumulated liability.

18 Duration and Termination

This Agreement shall remain in force until the Main Agreement is terminated, or until terminated by the Customer according to the terms of this Agreement. Upon termination of this Agreement, Benelizer's obligations remain valid for as long as data is in its possession.

Benelizer's authorization to process Personal Data on behalf of the Customer ends at the termination of the Main Agreement.

If a Party is guilty of material breach of this Agreement, the other party is entitled to terminate the Agreement in writing with immediate effect. Breach of applicable rules for processing personal data and violation of the Data Controller's instructions will always constitute a material breach.

19 Changes

This Agreement may change over time in order to adapt to best practices or to adapt to changes to rules and regulations. Customers will be informed about new versions of this Agreement before it can take effect, and the Customer must agree in writing to the changes. If the Customer cannot accept the changes, the Customer can terminate the Agreement.

---------- ---------- ----------

APPENDIX 1 to the DATA PROCESSOR AGREEMENT

Security and Data Safety Measures

A) Passwords and Access to the Benelizer Web Application (The Application)

1. It is possible to enable a forced change of password after the first login to The Application.

2. A password can only be saved when it has 6 to 20 characters which contain at least one numeric digit, one uppercase and one lowercase letter.

3. Passwords are one-way encrypted and once created they cannot be viewed or printed from The Application or directly from database records.

4. Every log-in attempt to The Application is recorded in a read-only log with a timestamp, IP-address and whether the password was correct or not. After 5 consecutive wrong passwords the user will be blocked from further log-in attempts.

B) Backup of Data

All data are backed up on a regular basis.

- Hourly in 336 versions (14 days)
- Daily in 31 versions (1month)
- Monthly in 11 versions (1 year)

C) Firewall and Anti-virus

- The servers are protected by a maintained firewall.
- The servers are protected by maintained anti virus/ransom/malware software.

d) Security of IT Systems and the Handling Procedures

1. The backup and restore system is verified on a regular basis.
2. Transmission of personal data shall be by using encryption (VPN or HTTPS).
3. Only high-quality hardware and software are used, and is continuously updated with security updates.
4. It is ensured that physical and electronic access control are in force. Only employees with work-related needs have access to the personal data and this access does not give any further rights to processing the information than necessary.
5. Access Management covers all phases of an employee's employment, including user access, periodic checking of user rights at least once a year, change of user rights as needed and termination of user access.
6. Formal procedures and processes are in place for dealing with personal data security breaches.
7. Procedures are in place for regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to handle security.
8. Employees receive appropriate training, adequate instructions and guidelines for processing personal data.
9. It is ensured that Employees involved in the processing of personal data are familiar with the security requirements and are subject to confidentiality
10. Physical access and electronic access to personal data is approved by the persons authorised for this task.
11. Only authorized persons have access to the data processor's buildings and physical access rights must be involved when the need arises.
12. Buildings used for data processing are secured against break-in with professional alarm systems and surveillance equipment at a level according to the risk of the data processing of personal data.
13. There are internal guidelines in place that prohibit the printing of personal data and physical material with personal data is kept locked when not used so that these are not available to unauthorised persons.
14. Personal data may not be brought outside the data processor's locations.
    For home or remote workplaces these rules are in force:
    - Printing or saving of personal data to home/remote storage devices is not permitted.
    - Communication with servers is always encrypted.
15. Employees with data access are required to lock their screen when it is left (PC, portable, iPad, mobile, etc.). The locking requirement also applies to remote and home workplaces.
16. Personal data may not be stored locally on PCs or other endpoint devices, but must be stored centrally on servers located in a secure server room.

17. When discarding personal data equipment, data must be deleted effectively using an erase program, or the storage media must be destroyed in such a way that it is no longer readable.
18. There are formal procedures in place for change management in IT systems and IT equipment. The procedures are conducted in order to ensure that any change is duly documented, authorized, tested and approved prior to implementation.
19. Benelizer, or Benelizer's customers, can - if it is necessary - choose to initiate and participate in a compliance inspection/audit at the sub-contractor. Such a request must be given with reasonable notice and the Customer must carry the cost for time spent – at a reasonable cost - by the sub-contractor during the inspection/audit.

- - - - - - - - - - - - - - - - - -

APPENDIX 2 to the DATA PROCESSOR AGREEMENT

The Nature of the Personal Data Processed

The Benelizer application uses personal data to create and maintain information about users with access to the Benelizer application and/or users who act as respondents to the questions issued by the Benelizer application.

The following data is created and maintained for each user – the items in bold are mandatory.

- **Name**
- **Email**
- **Is internal or external user**
- **Password**
- **Wrong password count**
- **Login count**
- **Last login date**
- **Login log**
- **Access rights to the application**
- Initials
- Salutation
- Title
- Office
- Department
- Telephone
- Mobile
- Skype ID
- Key dimension access (limitations in data access)
- Qualifications for answering to questions

For users with access to the Benelizer application a timestamp is saved with the user's name on records being created or updated by the user.

For users who act as respondents to the questions issued by the Benelizer application their replies are recorded.

- - - - - - - - - - - - - - - - - -