

Article 1. Definitions

1.1. Mindtime Backup: Mindtime Backup B.V. registered with the chamber of commerce under number 51172313.

1.2. User software: Online backup programming from Mindtime Backup, used for storing digital data. The digital data is sent to the Mindtime Backup server by the user through a communication channel, by means of the user software.

1.3. User: the natural person or legal person who has accepted the Mindtime Backup user terms and conditions and a client of Mindtime Backup by Supplier.

1.4. Pro Backup: Backup account for one or multiple PCs / laptops / servers with standard backup modules including Exchange, (MY)SQL, Sharepoint, VMWare, Lotus Notes en Oracle.

1.5. PC Backup: Backup Account for 1 PC or laptop.

1.6. VM Backup: Backup Account as Pro Backup. However, VM Backup is only single stored.

1.7. Documentation: Information, brochures, instructions and manuals for the User, provided by the supplier along with the user software and/or goods.

1.8. Supplier: The supplier of the user software for the user.

Article 2. Acceptance of the user terms and conditions

2.1. The user agrees to the user terms and conditions by accepting the user terms and conditions during the installation of the user software.

Article 3. Rights/Obligations Mindtime Backup

3.1. Mindtime Backup or her suppliers have the right to alter the user software from time to time in order to improve the functionality and correct errors. If a modification leads to a significant change in functionality, the supplier will inform the user of this modification. Because the user software is supplied to multiple users, it is not possible for one user to refuse a certain modification. Mindtime Backup or the supplier is not obliged to compensate for any damage caused during the modification of the user software.

Article 4. Conditions of the User software

4.1. User is obliged to follow the instructions as stated in the Documentation strictly.

4.2. Unless agreed otherwise in written form, the user is responsible for the installation and configuration of the user software in accordance with the Documentation.

4.3. The user determines which digital data is stored by means of the user software. Mindtime Backup has no knowledge of this digital data. The user is also obliged to ensure that the data is lawful and that it does not infringe the rights of any third parties. The user will safeguard Mindtime Backup against any claims made by third parties that are based upon the proposition that the user has stored unlawful digital data using the user software.

4.4. If Mindtime Backup should discover that digital data stored by the user by means of the user software is unlawful, Mindtime Backup will take immediate action in order to remove this data or block access to it. In such a case, Mindtime Backup also has the right to block access to or remove the user's digital data. This in accordance with Mindtime Backup's judgement. In no case will Mindtime Backup be held liable for any damage that may come forth out of this act.

4.5. The user is to keep the usernames and passwords provided by the supplier strictly confidential. Mindtime Backup or the supplier is not responsible for abuse of user names and passwords and may assume that the user that logs in, is indeed the user. The user is to inform the supplier if the user suspects that user names and passwords have fallen into the hands of unauthorised persons. Mindtime Backup or the supplier has the right to take effective action in such cases.

4.6. The user is to refrain from any unauthorised use of the user software and will behave in accordance with what Mindtime Backup or the supplier may expect from a careful manager of the user software.

4.7. Neither Mindtime Backup nor Supplier are liable for any damage that may come forth out of the loss of the encryption key by the user, or that a third party may have gained access to the encryption key, thus providing him with access to the user's digital data.

4.8. The user is responsible for keeping and safeguarding the encryption key, and is aware that by destruction or loss of the encryption key, the data stored with Mindtime Backup will become unusable and unreadable.

4.9. The user will safeguard Mindtime Backup from all damage and any claims from third parties arising from breach by the user of the guarantees and/or statements made by the user in the previous paragraph.

Article 5. Rights of intellectual property

5.1. All intellectual property rights on the user software belong solely to Mindtime Backup. User only receives a right of use that is not exclusive, nor transferable, and authorisations that are expressly granted with these conditions or in any other way and for all other, the user will not duplicate or make copies of the user software, excepting one spare copy for personal use.

5.2. The user is not permitted to remove of change any indication of copyright, brands, trade names or any other rights of intellectual property from the user software or the manuals.

5.3. Mindtime Backup is allowed to take technical measures in order to protect the user software programming. If Mindtime Backup has used technical means to protect the user software, the user is not allowed to remove or avoid this protection.

5.4. In case of termination or interim dissolution of the user conditions, the User will remove or destroy all the user software and Documentation and all copies.

Article 6. Liability, Warranty and Indemnity

6.1. The User may only claim a warranty if he or she has fulfilled all his or her obligations towards Mindtime Backup and/or the Supplier.

6.2. If the User fails to fulfil all of his or her obligations towards Mindtime Backup and/or the Supplier, Mindtime Backup may suspend the granted Mindtime Backup warranty until the User has fulfilled all of his or her obligations towards Mindtime Backup and/or the Supplier.

6.3. Each liability of Mindtime Backup and/or the Supplier is per event — whereby a related set of events counts as single event — limited to compensation for direct damages up to the amount that the relevant liability insurance covers or up to the amount corresponding to the amount in the past 6 months actually paid by the User to the Supplier (excluding VAT).

6.4. The liability of Mindtime Backup and/or the Supplier for indirect damages, including consequential losses, loss of revenue and profit, lost savings, intangible damage and damages due to company stagnation is excluded.

6.5. The liability of Mindtime Backup and/or the Supplier for direct damages, including damages resulting from failure to reach an agreed deadline, including through force majeure, staff or freelancers' failures, is excluded.

6.6. The User indemnifies Mindtime Backup and the Supplier against any third party claims for any damages, costs or interest relating to User Software and/or Agreements between the User with Mindtime Backup and/or the Supplier.

6.7. Mindtime Backup and/or the Supplier is never liable for damages caused by cyber terror or attacks by internet hackers.

6.8. Any right to compensation is conditional upon the User notifying Mindtime Backup and/or the Supplier in writing within two weeks of such an occurrence, in the absence of which this right expires.

6.9. The User indemnifies Mindtime Backup for the data selection for the backup from the User. Also if these Data are corrupted, infected or encrypted.

Article 7. Data storage

7.1. The backed up data from user are first compressed and encrypted before they are stored in 2 secured data centres of Mindtime Backup.

7.2. The Pro Backup Data is stored on two physical locations.

7.3. The PC Backup Data is stored on two physical locations.

7.4. The VM Backup Data is stored on one physical location. This is called single storage by Mindtime Backup.

Article 8. Force Majeure

8.1. In case of a force majeure situation, meaning in any case malfunctions or failure of the internet, the telecommunication infrastructure, of any operator or internet service or access provider, the full occupation of dialup lines or insufficient bandwidth of an access provider, domestic disturbances, mobilisation, war, disruption in transport, company malfunctions, interruption in supply, fire, flood, in and export impairment, and in the event that Mindtime Backup cannot reasonably be expected by its own suppliers to fulfil the user conditions, the implementation of the user conditions will be suspended or terminated if the force majeure situation takes longer than 30 days, all without any obligation to compensation.

Article 9. Duration and termination

9.1. The user conditions are entered into for at least 12 (twelve) months and can only be terminated as determined in these user conditions. Without termination, the user conditions are implied for an equally long period without notice.

9.2. A party may terminate the user conditions in compliance with 2 (two) months notice. For this, the termination form has been filled in and should be in Mindtime Backup's possession at least two months before the expiry of the contract year.

9.3. If a party does not meet certain obligations that come forth out of the user conditions properly or within a prescribed period, the party in question is in default and the other party is entitled to terminate the user conditions partially or entirely without notice, without prejudice to the other rights of the dissolving party and without the dissolving party being liable for damage.

9.4. In case of a dissolution or termination, as specified in the preceding articles, the following obligations will remain standing after the expiry of the user conditions:

- Intellectual property rights;
- Liability, Warranty and Indemnity

These will continue for as long as Mindtime Backup or the Supplier can reasonably presume the continuance of these.

Article 10. Changes terms and conditions

10.1. Mindtime Backup reserves the right to alter or make additions to these terms and conditions.

10.2. If the user does not want to accept a change in these conditions, he can state this within 30 days prior. In this case the already closed terms and conditions stay valid. Mindtime Backup can terminate this agreement in accordance Article 9.2.

Article 11. Final Provisions

11.1. These user terms are governed by Dutch law.

11.2. Changes in management or business entity are of no influence on these user conditions.

11.3. As far as not otherwise specified by the mandatory rules of law, all disputes that may arise from the user conditions will be submitted to the competent Dutch court in Zwolle.

11.4. Partial Invalidity:

If a certain provision in these user conditions turns out to be invalid, this does not influence the validity of the entire user conditions.

Parties will establish (a) new provision(s) in replacement, which will resemble the intent of the original user conditions as far as legally possible..

Article 12. Confidential Information and Privacy

12.1. Mindtime Backup and the User ensure that all information received from the other party, known or should be known to be confidential, remains secret, unless a statutory duty requires disclosure of such information. The party receiving confidential information will only use it for the purpose for which it is provided.

12.2. User indemnifies Mindtime Backup against claims from persons whose personal data are registered or processed in the context of a personal registration done by the User or for which the User is otherwise responsible under the law unless the User proves that the facts of the claim are attributable only to Mindtime Backup. By signing these Terms of Use, the User agrees with the provisions contained in the attached Data Processing Agreement.

Contact details

If you have any questions or comments after reading these user conditions, feel free to contact us by mail or e-mail.

Signature User

Name:

Company:

Function:

Date:

Signature:



Data Processing Agreement

The undersigned:

- I. Mindtime Backup B.V., with registered offices and place of business in Deventer (the Netherlands) at the Schonenvaardersstraat 14N, legally represented in this matter by Roy Wichink Kruit, hereinafter referred to as: 'the Processor';

and

- II., with registered offices and place of business in at, legally represented in this matter by, hereinafter referred to as: 'Data Subject';

Take the following into account:

- Data Subject and the Processor have concluded an accord for the provision of services described in an agreement concluded between the two parties, which results in, or may result in, third party Personal Data being made available by Data Subject to the Processor.
- The parties conclude this Data Processing Agreement to confirm that they will carry out all activities in accordance with any legal provisions.

The parties declare to have agreed as follows:

Article 1. Definitions

The words or phrases used in this agreement have the following meanings:

- *Concerned party*: the person to whom any personal data relates.
- *Underlying Agreement*: the Contract in which Data Subject has instructed the Processor to process personal data to which the General Terms and Conditions may also apply.
- *Agreement*: this Data Processing Agreement.
- *Personal Data*: Any data relating to an identified or identifiable natural person that the Processor will process or shall process subject to the Underlying Agreement.
- *Process/Processing*: All actions or series of actions performed on Personal Data, whether or not by automated means, such as: collecting, documenting, storing, customising, using, combining and/or destroying.
- *General Terms and Conditions*: the Processors' Terms of Use.

Article 2. Applicability

2.1. Unless otherwise agreed in writing by the parties, the provisions of this Agreement shall apply to any Processing by the Processor subject to the Underlying Agreement.

2.2. The provisions of this Agreement prevail over the Underlying Agreement and, potentially, apply to the implementation of the General Terms and Conditions applicable to the Underlying Agreement, as far as it concerns the processing of Personal Data.

Article 3. Processing by the Processor

3.1. The Processor processes the Personal Data exclusively on behalf of Data Subject in the performance of the work as defined in the Underlying Agreement, subject to any contrary legal obligations, in accordance with the provisions of the Personal Data Protection Act and the General Data Protection Regulation (GDPR) applicable from 25 May 2018. The Processor will not process the personal data for any purpose other than as defined in the Underlying Agreement, subject to any contrary legal obligations.

3.2. Employees of the Processor shall be granted access to the Personal Data only to the extent necessary for the execution of the Underlying Agreement.

3.3. The Processor may process Personal Data outside the Netherlands exclusively with the prior written consent of Data Subject.

3.4. The Processor will not disclose Personal Data to third or concerned Parties unless they have the prior written consent of Data Subject or because of statutory obligations. In the case of legal obligations, the Processor will inform Data Subject as soon as possible.

3.5. The Processor shall enable Data Subject to comply with statutory obligations at all times, in particular the rights of the Concerned Parties, such as, but not limited to, a request for inspection, improvement, addition, removal, or protection of Personal Data and performing a granted registered objection.



Article 4. Data-leakage reporting requirements

4.1. The Processor will inform Data Subject as soon as possible after the first discovery of all (suspected) security breaches and any other incidents that may relate to the Personal Data and by law that must be reported to the Supervisor or Concerned Person(s), without prejudice to the obligation to reverse or limit the consequences of such infringements and incidents as soon as possible. In addition, at the first request of Data Subject, the Processor will provide all information deemed necessary by Data Subject to assess the incident.

4.2. The Processor has a thorough plan of action on dealing with and handling breaches and will provide Data Subject, at their request, with access to the plan.

4.3. The Processor will leave the reporting to regulatory bodies to Data Subject.

4.4. The Processor will provide all necessary cooperation and additional information to the regulatory bodies and/or the Concerned Person(s) as soon as possible.

4.5. The Processor keeps a detailed log of all (suspected) security breaches, as well as the actions taken following such infringements and provides it at the first request of Data Subject.

4.6. Reporting by the Processor or Data Subject of data leaks to the competent authorities, subject to statutory obligation, can never lead to imputable failures or accusations of unlawful conduct against the other party.

Article 5. Safeguards and inspection

5.1. The Processor takes all measures to protect Personal Data against loss or unlawful access. These measures are described in the Underlying Agreement and in the applicable Terms and Conditions and working processes of the Processor and ensure an appropriate level of security in processing Personal Data.

5.2. The Processor allows Data Subject to inspect or allows an inspection agency, which is neutral and expert according to objective criteria, to inspect for the Processor's compliance with security measures. Data Subject precedes the Processor in ensuring that the inspection agency practices strict confidentiality regarding third parties, subject to any legal obligation(s), bears the costs of inspection and provides the Processor with a copy of the result of the inspection.

Article 6. Obligations of Data Subject / consent

6.1. Data Subject ensures that the processing of Personal Data is in accordance with this Agreement, and the Underlying Agreement, and does not conflict with the current Data Protection Act and/or the General Data Protection Regulation (GDPR) applicable from 25 May 2018.

6.2. The 'prior written consent' of Data Subject as referred to in this Agreement is applicable in part if having such consent is clearly indispensable to the processor to fulfil their obligations subject to the Underlying Agreement.

Article 7. Liabilities

7.1. The Processor is liable for damages resulting from or related to non-compliance with this Agreement.

Article 8. Engagement of third parties

8.1. The Processor is only entitled to outsource the execution of the work wholly or in part to third parties.

8.2. In these cases, the Processor will remain the point of contact and be responsible for compliance with the provisions of this Data Processing Agreement.

8.3. The Processor may only process the personal data in the European Union. Transmission to other countries is only permitted after the prior written consent of Data Subject and in compliance with the applicable laws and regulations.

8.4. The Processor keeps an up-to-date register of third parties engaged that includes their identities, locations, and descriptions of the activities of the third parties.

Article 9. Terminations

9.1. This Agreement has been concluded for an indefinite period and ends by law at the time when the Underlying Agreement terminates, or at least when the Processor has fulfilled their obligations arising from the Underlying Agreement.

9.2. Except if otherwise stated in writing by Data Subject, the Processor will, in the event of termination of the Agreement, immediately return all of the Personal Data made available to them to Data Subject and destroy all digital copies of any Personal Data, with written confirmation thereof given to Data Subject, subject to legal obligation(s) for the Personal Data to be retained for a certain period of time.



Article 10. Confidentiality obligations

10.1. Persons employed by or acting on behalf of the Processor, as well as the Processor themselves, are required to maintain confidentiality with respect to any Personal Data, of which they may be aware, except to the extent of provision required by law.

10.2. If, on the basis of a legal obligation, the Processor is required to provide data, the Processor will verify the basis of the request and the identity of the applicant and the Processor will immediately inform Data Subject, prior to disclosure, unless legal requirements prohibit it.

Article 11. Divisibility

11.1. If one or more provisions in this Agreement appear to be unlawful and/or prove to be, the remainder of the Agreement will remain in force. The parties will consult on the provisions that are not valid in order to make a replacement arrangement that is valid and to the greatest possible extent covering the same scope of the regulation to be replaced.

Article 12. Applicable law and disputes

12.1. Dutch law applies to this Agreement.

12.2. All disputes arising out of or related to this Agreement will be submitted only to the Overijssel Court, Zwolle.

Thus agreed upon and signed in duplicate,

Date:

Place: Deventer

Place:.....

Name: Roy Wichink Kruit

Name:

On behalf of the Processor

On behalf of Data Subject