OMNIPRIVACY

OMNIPRIVACY Terms

(as of 09.11.2023)

OMNINET company (“**OMNINET**”):

- Means in **Belgium**: OMNINET Technologies NV, Diestsevest 32 bus 2a, B-3000 LEUVEN, Belgium, omniprivacy@omninet.be, www.omniprivacy.be
- Means in **Netherlands**: OMNINET Nederland, President Kennedylaan 19, NL-2517 JK Den Haag, Netherlands, omniprivacy@omninet.nl, www.omniprivacy.nl
- Means in **Germany**: OMNINET Software-, System- und Projektmanagementtechnik GmbH, Dr.-Otto-Leich-Straße 3, D-90542 Eckental, Germany, sales@omninet.de, www.omniprivacy.de
- Means in **Austria**: OMNINET Austria GmbH, Engerthstraße 90 / 1-6, 1200 Wien, Austria, sales@omninet.at, www.omniprivacy.eu
- Means in **Switzerland**: OMNINET GmbH (Schweiz), Seedammstrasse 3, 8808 Pfäffikon, Switzerland, contact@omninet.ch, www.omniprivacy.eu
- In all **other countries** this means: OMNINET will select any seat from the OMNINET companies mentioned above from which for example the invoicing of SaaS Service will be performed.

1 Scope of applicability

1.1 These license terms apply to contracts between the customer and the OMNINET country subsidiary (hereinafter "**Provider**") for the temporary provision of the OMNIPRIVACY software as part of a Software as a Service (SaaS) solution.

1.2 By accessing or using the services under this agreement, or authorizing or permitting any user or end-user to access or use the services under this agreement, the customer agrees to be bound by these terms.

1.3 If the customer does not agree with these terms, the customer must not accept these terms and may not access or use the services under this agreement.

1.4 These terms can be amended by Provider from time to time.

1.5 The customer OMNIPRIVACY sale agreement can be ordered via an OMNIPRIVACY Partner (hereafter “**Partner**”) or be ordered directly with Provider. These Terms are applicable for both these sale channels.

2 Subject matter of the agreement

2.1 The Subject matter of the agreement is the transfer of the Contractual Software of the Provider for use via the Internet and the granting of storage space on the servers of the Provider ("**SaaS Service**").

2.2 The Provider may include subcontractors when granting storage space. The use of subcontractors does not relieve the Provider from its sole obligation to fulfil the contract towards the customer completely.

2.3 The Provider is not responsible for the preparation and maintenance of the data connection between the IT system of the customer and the servers of the Provider.

3 Definition of the Contractual Software

3.1 OMNIPRIVACY is a cloud provisioned GDPR- and Privacy Management application. Cloud provisioned means that the customer requires a web browser and an Internet connection to connect to OMNIPRIVACY (hereinafter „**Contractual Software**“).

3.2 The functional scope of the Contractual Software results from **Appendix 1 – SaaS Service Performance Description**.

4 Surrender of the Contractual Software

4.1 For the duration of the contract, the Provider provides the Customer with the latest version of the Contractual Software via the internet against remuneration. For this purpose, the Provider sets up the Contractual Software on a server, which is accessible for the customer via the internet.

4.2 The Provider immediately eliminates all software errors according to his technical possibilities. An error occurs if the Contractual Software does not fulfil the functions specified in the performance description (see **Appendix 1 – SaaS Service Performance Description**), gives erroneous results or otherwise does not function properly, so that the use of the Contractual Software is impossible or limited.

4.3 The Provider will continue to develop the Contractual Software and will improve it by ongoing updates and upgrades.

5 Rights of use in relation to the Contractual Software

5.1 The Provider grants the customer the non-exclusive and non-transferable right to use the Contractual Software as intended during the term of the Agreement as part of the SaaS Service.

5.2 Depending on the License Option (see chapter 17.1), license rights allows access to the software by a specific number of users (= Named User - specific user ID) or by a number of concurrent accesses (= Concurrent user – simultaneous access and independent from number of users).

5.3 The customer may only reproduce the Contractual Software if this is covered by the intended use of the software according to the current performance descriptions. Necessary duplication includes the loading of the Contractual Software into the main memory on the server of the Provider, but not even the temporary installation or saving of the Contractual Software on data carriers of hardware used by the customer.

5.4 The customer may only duplicate the user documentation for its own purposes.

5.5 The customer is not entitled to make the Contractual Software, including the user documentation and any other accompanying material, available for use by third parties against payment or free of charge. This applies in particular to a re-letting.

6 Granting of storage space

6.1 The Provider leaves the customer a defined storage space on a ‘server’ to store his data. The customer can store contents on this server a limited amount of volume as specified in ‘**Appendix 1 – SaaS Service Performance Description**’. If the storage space for storing the data should no longer be sufficient, the Provider will inform the customer about this. The customer can reorder appropriate allocations subject to availability at the Provider.

6.2 The Provider ensures that the stored data can be accessed via the Internet.

6.3 The customer is not entitled to provide the storage space to third parties for use in part or in full, against payment or free of charge.

6.4 The Provider is obliged to take suitable precautions against data loss and to prevent unauthorized access of third parties to the data of the customer. For this purpose, the Provider will make daily backups, check the data of the customer for viruses as well as installing state of the art firewalls.

6.5 In any case, the customer is exclusively entitled to the data and can export this data at any time via the functions contained in the administration area of the OMNIPRIVACY application.

6.6 In the event of termination of the contractual relationship, the customer is obliged to export the data stored in the application himself via the administration functions provided for this purpose until the end of the term.

6.7 The Provider has in terms of the data of the customer neither a right of retention nor the legal landlord lien.

7 Support

7.1 The scope of support is set out in "**Appendix 2: Support parameters**" of this Agreement.

8 Interruption / Impairment of accessibility

8.1 The customer may not be able to access or use the SaaS Service

- during planned downtime for upgrades and maintenance to the SaaS Service ("**Planned Changes**"), or
- during any unavailability caused by circumstances beyond OMNINET's reasonable control, such as, but not limited to, acts of God, acts of government, acts of terror or civil unrest, technical failures beyond OMNINET's reasonable control (including, without limitation, inability to access the internet), or acts undertaken by third parties, including without limitation, distributed denial of service attacks.

8.2 OMNINET will use commercially reasonable efforts to notify the customer in advance. For this notification the e-mail address will be used that is mentioned on the Order Subscription Form by Customer or Partner.

8.3 OMNINET will use commercially reasonable efforts to schedule Planned Changes outside Business Hours (Monday until Friday from 9AM until 5PM on official business days) of Provider's seat.

8.4 OMNINET guarantees an SaaS Service availability of 99,0%, measured on a monthly basis during Business Hours and excluding unavailability due to Planned Changes. This does not apply in the event of unforeseen impediments such as events of force majeure, mobilization, war, strikes, lock-outs, riots or other events for which OMNINET is not responsible.

9 Duties of the customer

9.1 The customer undertakes not to drop any content that infringes the law, regulatory requirements or third-party rights on the storage space provided.

9.2 The customer is responsible for the proper functioning of its own network infrastructure as well as the network or Internet connections that are required to access the Contractual Software. This includes in particular the availability, continuity, security and performance of the internet connection available to the customer for accessing the Contractual Software.

9.3 The customer is obliged to prevent the unauthorized access of third parties to the Contractual Software by taking suitable precautions. For this purpose, the customer will, as far as necessary, inform his employees about the compliance with the copyright.

9.4 Without prejudice to Provider's obligation to back up the data, the customer is responsible for entering and maintaining the data and information required using the SaaS Service.

9.5 The customer is obliged to check his data and information for viruses or other harmful components prior to entry and to use state-of-the-art anti-virus programs.

9.6 The customer will generate a "User ID" and password to access the use of the SaaS Service itself, for each individual user a unique User ID, which are necessary for the further use of the SaaS service. The customer is obliged to keep this access data secret and not to make it accessible to third parties.

9.7 Copyright and data protection laws may protect the content stored by the customer in the storage space. The customer hereby grants the Provider the right to make the content stored on the server accessible to the customer during his requests via the Internet and in particular to be able to reproduce and transmit it as well as to reproduce it for the purpose of data backup.

10 Remuneration

10.1 Unless agreed otherwise, except during the free trial period, all charges associated with the customer’s account (“**Subscription Charges**”) are due in full and **quarterly payable in advance** when the customer subscribes to the SaaS Service. The Subscription Charges are based on the License Option chosen by the customer (see chapter 17.1) and are payable in full until the SaaS Service is terminated according chapter 13. Any remuneration is in the form of net prices, excluding statutory VAT.

10.2 In case SaaS Service is contracted directly with Provider, the customer will receive an electronic invoice for each Subscription Charges from the Provider. The invoice will be emailed to the standard email address of the customer that was provided on the Order Subscription Form, unless a different email address has been provided.

10.3 In case SaaS Service is contracted via a Partner of the Provider (OMNIPRIVACY implementation partner), the customer will receive an invoice for each Subscription Charges from the Partner. The invoice will be emailed to the standard email address of the customer, unless a different email address has been provided.

10.4 Provider or Partner may, for its own convenience, use a third party service provider to manage payment processing.

10.5 Unless agreed otherwise all Subscription Charges are non-refundable. No refunds shall be issued for partial use or non-use of the SaaS Service by customer.

10.6 OMNINET will notify the customer if no or not complete payment was received within the due date for the customer’s account. If OMNINET does not receive payment within the foregoing time period, in addition to OMNINET’s right to other remedies available under law, OMNINET may:

- charge an interest for late payment @ 1.5% per month and/or;
- suspend the customer’s access to the storage space until OMNINET receives the customer’s payment towards the Subscription Charges as specified herein and/or;
- terminate the customer’s account in accordance with chapter 13.3.

10.7 The customer may upgrade or downgrade user licenses or upgrade or downgrade a License Option. The customer understands that downgrading a License Option may cause loss of content, features, or capacity of the SaaS Service as available to the customer before downgrading his account. OMNINET will not be liable for such loss. When the customer makes an upgrade or downgrade, the new Subscription Charges become immediately applicable. Upon upgrade, the new Subscription Charges for the subsisting quarter would be charged on pro-rated basis at the next invoice. Subsequent quarters will be charged in full according to the new Subscription Charges. Upon downgrade, from the next invoice period the Subscription Charge will be adapted.

10.8 Indexation: All prices and charges can be adjusted by OMNINET on **1st of January of each year** by applying an indexation specific to the customer's territory. Please note that within the **first 12 months** of the term there is **no indexation** possible.

- Indexation Belgium & Luxemburg territory:
  New Price = Old Price x [0.2 + 0.8 (new Agoria index / basic Agoria index)]
  - New Price: the adjusted price and rate,
  - Old Price: the initial price and rate (at the start of the term),
  - New Agoria index: the Agoria index applicable to the month of December prior to the date of indexation,
  - Basic Agoria index: the Agoria index applicable to the month prior to the month the OMNIPRIVACY subscription started,
  - The Agoria index: the "Agoria Digital" index is utilized (= new index provided by Agoria since August 2022, specifically for the digital sector).
- Indexation Netherlands territory:
  - The index figure will be calculated using the Dutch CAO (Collective Labour Agreement) wages per month, as published by the Dutch C.B.S. (Central Bureau of Statistics), index "Zakelijke en ICT-dienstverlening" (index J-62 "IT-dienstverlening"), or should this publication be ended, the most comparable C.B.S. figure.
  - https://www.cbs.nl/nl-nl/cijfers/detail/83854NED
- Indexation German territory:

  The index figure will be calculated using the Germany published consumer price index by the Federal Statistical Office or should this publication be ended, the most comparable consumer price index figure.

11 Additional Services

11.1 All services provided on request of the customer but not included in this contract and its annexes are considered as additional services.

11.2 The customer must remunerate additional services separately. In this case, the parties will make a separate agreement.

12 Warranty and liability

12.1 The Provider guarantees the functional and operational readiness of the SaaS Service in accordance with the provisions of this agreement.

12.1 In the event that the services of the provider are claimed by unauthorized third parties using the customer's access data, the customer shall be liable for resulting fees in the context of civil liability until receipt of the customer's order to change the access data or customer's notification of loss or theft if the customer is at fault for the access of the unauthorized third party.

12.2 The Provider is entitled to block the storage space immediately if there is a reasonable suspicion that the stored data is unlawful and / or infringes the rights of third parties. A reasonable suspicion of unlawfulness and / or infringement of rights exists in particular if courts, authorities and / or other third parties inform the Provider thereof. The Provider must notify the customer of the blockage and the reason for this immediately. The blockage should be cancelled as soon as the suspicion is invalidated.

12.3 Claims for damages against the Provider are excluded, irrespective of the legal grounds, unless the Provider, its legal representatives or vicarious agents have acted intentionally or with gross negligence.

12.4 For slight negligence, the Provider is liable only if an essential contractual obligation by the Provider, its legal representatives, officers or vicarious agents was violated. The Provider is only liable for foreseeable damages that typically have to be expected. Essential contractual obligations are those obligations, which form the basis of the contract, which were decisive for the conclusion of the contract and on the fulfilment of which the customer may rely.

12.5 The Provider is liable without limitation for intentional or negligent damage caused by injury to life, limb or health by the Provider, its legal representatives or vicarious agents.

12.6 The Provider is only liable for loss of data to the extent that lost data can be restored with reasonable costs.

13 Term and termination

13.1 The SaaS Service shall have a term of twelve (12) months, commencing on the date of delivery of the SaaS Service. The delivery of the SaaS Service is the date of delivery of the login details of the SaaS Service.

13.2 **After the first 12 months**, the SaaS Service can be effectively **terminated at three months' notice to the end of a calendar month**. The customer can terminate the SaaS Service by sending an email or by registering the termination online. This termination is **only valid** when the notice email of the customer is **confirmed** by Provider within two business days.

13.3 In addition to suspension for late payment or non-payment of Subscription Charges, Provider may suspend the access to and use of the SaaS Service if the customer is in violation of these terms. Provider will notify the customer of the activities that violate these terms and, at Provider's sole discretion, provide the customer with a reasonable period to cure or cease such activities. If the customer does not cure or cease such activities within this cure period or if Provider believes that the customer's breach of these terms cannot be cured, the customer's account shall be terminated.

13.4 The right of each contracting party to terminate the contract for cause without notice remains unaffected. The Provider is entitled to terminate the contract without notice in particular if the Customer does not make due payments despite a reminder with a grace period or violates the contractual provisions for the use of the SaaS Service. A termination without notice requires in any case that the other party is reminded in writing and asked to eliminate the alleged reason of termination without notice within a reasonable time limit.

13.5 Effect of termination:

- ➢ Data Export: Provider strongly recommends the customer to export all service data before terminating his account. In any event, following the termination of the customer's account either by the customer or Provider, unless agreed otherwise, service data will be retained for a period of one (1) week from such termination ("**Data Retention Period**") within which the customer may contact Provider to receive a copy of his service data. Beyond such Data Retention Period, Provider shall delete all service data in the normal course of operation. Service data cannot be recovered once it is deleted.

- ➢ Charges: If the customer terminates his account prior to the end of the then-effective subscription term or Provider effects such termination, in addition to other amounts, the customer may owe Provider, the customer must immediately pay any then unpaid charges associated with the remainder of such subscription term, unless waived by Provider in writing. This amount will not be payable by the customer in the event the customer terminates the SaaS Service as a result of a material breach of these terms by Provider, provided that the customer provides advance notice of such breach to Provider and affords Provider not less than thirty (30) days to reasonably cure such breach.

14 Data protection and secrecy

14.1 The Provider will comply with the provisions of the General Data Protection Regulation and in this connection will provide a processing agreement to be concluded with the customer (**Appendix 3 – Processor Agreement**). The customer is responsible for the consent declarations required by the provisions of the data protection laws by its customers and its contractual partners.

14.2 The Provider undertakes to maintain the strictest confidentiality with respect to all confidential information of the customer, in particular business or trade secrets, which he has come to know as part of the preparation, execution and fulfilment of this agreement, and to neither pass it on nor utilize otherwise. This applies to any unauthorized third party, also to unauthorized employees of both the Provider and the customer, if the disclosure of information is not necessary for the proper fulfilment of the obligations of the Provider under this contract. In cases of doubt, the Provider will allow the customer to give consent before such disclosure.

14.3 The Provider undertakes to agree with all employees and subcontractors whom he has set up in connection with the preparation, execution and fulfilment of this agreement, a provision identical in content to the above chapter 14.2.

15 Applicable law, place of jurisdiction

15.1 This contract is subject to the **laws** of the seat of the Provider. The provisions of the United Nations Convention on Contracts for the International Sale of Goods (CISG) are excluded.

15.2 Exclusive **jurisdiction** for all disputes arising from this contract is the seat of the Provider. The Provider can also sue the customer at his seat.

16 Miscellaneous

16.1 Attachments referred to in this agreement are part of the contract.

16.2 The Provider is entitled to include the name of the customer and other publicly available information in a reference list, which is also published on the internet. Other advertising notices must be agreed in advance with the customer.

16.3 The transfer of rights and obligations under this contract by the customer to a third party requires the prior written consent of the Provider.

16.4 The customer can only set off against such claims against the Provider that are undisputed or legally binding.

16.5 The customer is not entitled to exercise a right of retention against the Provider because of another claim not originating from this contract, unless this is undisputed or legally binding.

16.6 Amendments and additions to this agreement will only be effective if they are set out in an amendment signed by both parties. This also applies to the change of this written form requirement.

16.7 The ineffectiveness of one or more provisions of this contract shall not affect the validity of the remainder of the contract. The parties undertake to replace the ineffective provision with an effective provision which comes as close as possible to the economic purpose pursued by the invalid provision. Until such a provision, the ineffective provision shall be replaced by a provision that comes closest to the invalid provision from the economic point of view and purpose. The same applies in the event of a gap in the contract requiring a regulation.

16.8 Use of statistics: Provider is permitted to count visits and utilization of the software, so it can measure and optimize the performance of the software. This also helps the Provider to know which features are the most and least popular and see how users move around the software. All the information collected is aggregated and therefore anonymous.

17 Appendixes

17.1 Appendix 1 – SaaS Service Performance Description

Introduction

OMNIPRIVACY is a Cloud provisioned GDPR Management application.

Cloud provisioned means that the customer requires only a Web Browser and an Internet connection to connect to OMNIPRIVACY.

License Options

OMNIPRIVACY is available in three different licensing options ("**License Option**"):

1. OMNIPRIVACY Essential
2. OMNIPRIVACY Extended
3. OMNIPRIVACY Enterprise

OMNIPRIVACY Essential includes the following processes:

- 2x named users as DPO;
- 2x named users as Process Owners;
- 50x concurrent users for Self Service Portal;
- Breach Incidents;
- Privacy Requests;
- Processing Activities;
- Data Protection Impact Analysis (DPIA) - Light Process
- Document Templates;
- Contract Management;
- End-user Self Service Portal;

OMNIPRIVACY Extended includes the following processes:

- All processes of Essential
- 2x named users as DPO;
- 2x named users as Process Owners;
- 100x concurrent users for Self Service Portal;
- Data Protection Impact Analysis (DPIA) – Extended Process
- Data Transfer Impact Analysis (DTIA)
- Task driven follow-up;
- DPO Notes;
- Risk Management;
- Dashboards;
- Hookups (interfacing);
- Personalized End-user Self Service Portal;

OMNIPRIVACY Enterprise includes the following processes:

- All processes of Extended
- 5 x concurrent users as DPO and/or Process Owners
- 100x concurrent users for Self Service Portal;

The customer can subscribe to additional individual named DPO- and named Process Owner licenses (only for Essential and Extended license option), or to additional Concurrent User licenses (only for Enterprise license option) on top of the selected License Option.

Provider has the right to adapt its Contractual Software from time to time to align with market and customer requirements.

Product features:

- OMNIPRIVACY is a GDPR Management system to manage the following main GDPR processes:
  - Breach Incidents
  - Privacy Request
  - Record of Processing Activities
  - Data Protection Impact Analysis (DPIA)
  - Data Transfer Impact Analysis (DTIA)Processing Agreements
- OMNIPRIVACY will have regular updates. All OMNIPRIVACY customers will be automatically upgraded.
- The upgrades will be scheduled with specific release windows, where OMNINET will deploy the latest version of OMNIPRIVACY.
- OMNIPRIVACY will come with 3 specific user types:
  1. DPO User: The DPO user(s) have full access to the OMNIPRIVACY application system.
  2. Process Owner User: The Process Owner user(s) are expected to work on specific processes within OMNIPRIVACY. Therefor they will have limited access to the OMNIPRIVACY application system.
  3. End User: an end-user can log and follow-up its own Privacy Requests and Breach Incidents in the included Self Service Portal.
- For each legal entity of the customer an OMNIPRIVACY subscription is required. Every organization which acts as a GDPR Data Controller will use a separate OMNIPRIVACY subscription.
- A more detailed functional description of OMNIPRIVACY can be found in the OMNIPRIVACY Manual which will be amended from time to time.
- Languages:
  During login the user or end-user can select a language. OMNIPRIVACY is currently available in the following languages:
  - English
  - Dutch
  - French
  - German

Included Cloud Services:

The OMNIPRIVACY solution is provisioned using cloud services. These Cloud Services consist out of the following services:

- Accessibility
  - Accessibility via secure internet connectivity (https)
- OMNIPRIVACY components to operate OMNIPRIVACY
  - Network infrastructure
  - Server Hardware infrastructure
  - Operating System (incl. licenses)
  - Database System (incl. licenses)

  - OMNITRACKER Core System
  - OMNIPRIVACY Application based on the Contractual Software
- Security Services
  - Firewall Services including Antivirus, Web Filtering, Application Control, IPS, DoS and DDoS Protection
- Storage Space:
  - The customer can store contents up to a standard volume of 10 GB on his Contractual Software (database and attachments).
- Maintenance Services
  - Provisioning and Monitoring of the OMNIPRIVACY components
- Support Services
  - See chapter 17.2 (Appendix 2: Support parameters)
- Backup and Disaster Recovery Services

	Objectives
Recovery Point Objectives	
Application Data	<= 1 hour
Attachments	<= 24 hours

	Objectives
Disaster Recovery Time Objectives (*) (*) Within Business Hours	< 4 hours (**) (**) The recovery time does not apply when restoring a backup. This is because the time it takes to restore a backup depends entirely on the size and retention period of the backup.

- Customer confirms that Provider has the right to adapt this SaaS Service from time to time to align with market and customer requirements.

17.2 Appendix 2: Support parameters

OMNIPRIVACY Service Desk & Support:

- In case SaaS Service is contracted via a Partner of the Provider (OMNIPRIVACY implementation partner), then please contact your Partner for how to register for Service and Support.
- In case SaaS Service is contracted directly with Provider, please register your question or issue using the OMNIPRIVACY ticket registration tool or by sending an email to Provider (support.omniprivacy@omninet.be).

Severity levels and recovery target times:

OMNIPRIVACY Severity Level	Business Impact	Description of the impact	Example	OMNINET Recovery Target (workaround)
1	Major	Complete system down	Minimum 50% of user base is down; unable to perform any critical business functions.	< 4 hours
2	Medium	Degraded service of system, one process will not run, multiple critical users (10% of user base) cannot perform any useful work.	Unable to access a single key process of the Product; a large base of the users of the system is affected in their job; key users cannot work anymore.	< 8 hours
3	Minor	Normal user cannot perform any useful work, minor degradation to the service/process.	Can perform basic business functions on a limited basis; multiple users affected for a specific functionality that is not business critical.	< 3 business days
4	Minimal	Processes are working, but with inconveniences, process or function does not work optimal	Minor business impact, like performance not optimal but workable.	< 2 weeks

- “Recovery Target” is measured from the moment OMNINET received official registration by the Partner or from the moment OMNINET has received directly an official registration.
- “Recovery Target” is calculated on Business Hours and is based on the time OMNINET comes up with a workaround.
- The Recovery Target is an aim and OMNINET will do its utmost to reach the agreed Recovery Target, but these times cannot be guaranteed at all times. Waiting time for information or assistance from the customer or backup restore times are excluded.

Backup and Disaster Recovery Services:

- Recovery Point Objectives Application Data: <= 1 hour.
- Recovery Point Objectives Attachment Files: <= 24 hours.
- Disaster Recovery Time Objectives: < 4 Business Hours.
  PS: The Recovery Time does not apply when restoring a backup. This because the time to restore a backup depends entirely on the size and retention period of the backup.

17.3 Appendix 3 – Processor Agreement

17.3.1 Parties to the Agreement

The Controller: the customer (the SaaS Services customer)
The Processor: the Provider

17.3.2 Scope and Roles

17.3.2.1 This agreement applies to the processing of Personal Data, within the scope of the GDPR, by the Processor on behalf of the Controller.

17.3.2.2 For purposes of this Processor Agreement, customer and Provider agree that customer is the Controller of the Personal Data and Provider is the Processor of such data. In the case where customer acts as a Processor of Personal Data on behalf of a third party, the Provider shall be deemed to be a Sub-Processor.

17.3.2.3 These Terms do not apply where the Provider is a Controller of Personal Data.

17.3.3 Definitions

17.3.3.1 For the purposes of this Processor Agreement, the following definitions shall apply:

GDPR	Means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Personal Data	Means that data, meeting the definition of “personal data” as defined in Article 4 of the GDPR, which is provided by Controller to Processor in order to perform the processing as defined in Schedule 1 of this Processor Agreement.
Sub-Processor	Means a natural or legal person, public authority, agency or body other than the data subject, Controller and Processor who, under the direct authority of the Processor, are authorized to process Personal Data for which the customer is the Controller.

Terms used but not defined in this Data Processing Agreement (e.g., “processing”, “controller”, “processor”, “data subject”) shall have the same meaning as in Article 4 of the GDPR.

17.3.4 The Processing

17.3.4.1 The subject matter, duration, nature and purpose of the Processing, and the types of Personal Data and categories of data subjects shall be as defined in Schedule 1 of this Processor Agreement.

17.3.5 Obligations and rights of the controller

17.3.5.1 Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that Processing is performed in accordance with the GDPR. Those measures shall be reviewed and updated where necessary.

17.3.5.2 Where proportionate in relation to Processing activities, the measures referred to in paragraph 5.1 shall include the implementation of appropriate data protection policies by the Controller.

17.3.5.3 The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data are not made accessible without the individual's intervention to an indefinite number of natural persons.

17.3.6 Obligations of the Processor

The Processor shall:

17.3.6.1 process the Personal Data only on documented instructions from the Controller;

17.3.6.2 ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

17.3.6.3 take all measures required pursuant to Article 32 of the GDPR, namely to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of natural persons including, as a minimum, the measures set out in Schedule 2 of this Processor Agreement;

17.3.6.4 respect the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another Processor, namely that the Processor may not engage another Processor (Sub-Processor) without the prior authorisation of the Controller. Those Sub-Processors that are authorised by the Controller at the date of this processor Agreement are listed in Schedule 3. In cases where another Processor is engaged, the Sub-Processor must be subject to the same contractual terms as described in this Processor Agreement;

17.3.6.5 assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

17.3.6.6 assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, relating to security of Processing, Personal Data Breaches and data protection impact assessments;

17.3.6.7 at the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless applicable law requires storage of the Personal Data;

17.3.6.8 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;

17.3.7 Duration and Applicable Law

17.3.7.1 This Processor Agreement shall continue in effect for so long as the Processor is processing Personal Data on behalf of the Controller.

17.3.7.2 This Processor Agreement shall be governed by the laws of the registered office of Provider and subject to the exclusive jurisdiction of the courts of the registered seat of Provider for all disputes arising under this Processor Agreement.

17.3.8 Processor Agreement SCHEDULE 1 – Description of the Processing

Subject matter and duration of the Processing	The subject of the Processing is related to Provider software solution OMNIPRIVACY. OMNIPRIVACY could have in its databases Personal Data as mentioned in the type of Personal Data. The processing is limited to the validity of a contract between Controller and Processor. This contractual relationship is specifically related to an active Subscription of OMNIPRIVACY, more specifically the SaaS Services.

Nature and purpose of the Processing	The Processor processes additionally, directly or indirectly, the Personal Data in its Contractual Software and related SaaS Services.
Type of Personal Data and categories of data subjects	Controller and Processor acknowledge that this may imply the Processing of Personal Identifiable Information inside the SaaS Services databases as mentioned below: a. By default in OMNIPRIVACY no specific Personal Identifiable Information is processed. Besides: • First and Lastname of employees and users in OMNIPRIVACY • Business Phone and Email addresses of employees and users. b. It is possible to register free text and attachments in OMNIPRIVACY. These are generic input fields, so any kind of Personal Identifiable Information can be registered in OMNIPRIVACY by users.

17.3.9 Processor Agreement SCHEDULE 2 – Technical and Organisational Measures in accordance to GDPR Art. 32 (1) for Data Controller (Article 30 (1) (g)) and Data Processor (Article 30 (2) (d))

The security of customer‘s data is very important to the Processor. The Processor uses physical, electronic, and administrative safeguards that are designed to protect customer‘s data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

The following security measures are implemented by the Processor, to ensure the protection (Confidentiality, Integrity and Availability) of Personal Data:

1. **Pseudonymization**

   The Processor provides anonymization features, which Controller can request to anonymize the personal data. By using this feature, personal information within SaaS Services and the underlying databases may be modified to replace selectable combinations of personal information with an anonymous string.
   Restoring the anonymized data is not possible.
   The usage of this anonymization requests may be subject to fees.

2. **Encryption**

   All notebooks used by employees (e.g. technical staff involved in the provisioning of the SaaS Services) of Processor are individually protected by hard disk encryption (Microsoft Bitlocker).
   USB sticks or external hard disks, if used for the transport of personal data, are to be encrypted by the respective employee (Bitlocker To Go). This procedure was prescribed as a work instruction within the Provider.
   Backups made at Provider for data recovery purposes in the event of data loss are also encrypted. In addition, transfer of backup data is handled through an encrypted end-to-end connection.

3. **Ensuring confidentiality**

   a. Access and access regulations

The company building, where Provider is located, is equipped with an access control system with individual access (key) cards. The key assignment is regulated and documented and access lists are reviewed on regular basis. The different parts of the building are separated on a roll basis.
The Processor does not have a local server room. The Provider systems are hosted at a Subcontractor (see chapter “Processor Agreement SCHEDULE 3 – Sub-Processors”).

b. Access rules

Provider has established an authorization concept to differentiate Profiles, Roles, Transactions and Objects. It adheres to a Need-to-Know principle when granting access rights. These access rights can be evaluated.
The individual accesses, be it notification, change or deletion, are logged. The facilitation of Access Rights are documented.
Provider employees are regularly briefed on data protection law and are familiar with the procedures and user guidelines for Data Processing.
The password guidelines of Provider are based on the recommendations of the BSI in terms of length, password complexity, two-factor authentication, etc. For example resulting in a maximum password age of 90 days. A password change is periodically requested by the system. Two-factor authentication is enforced to access systems and applications by the Processor.
The Provider employees work with unique, personal user IDs. Group IDs are not used. In addition, all employees are instructed to lock their computers after a certain time (for example by screen saver) or whenever they are away from their computer.

c. Disclosure of data

Any transfer of personal data of the customer, e.g. copy of a database for the reproduction of reported issues as part of the support service, are carried in a secure way (e.g. copy of a database is encrypted and transferred in a secure way). There are regular reviews to ensure the integrity of transmitted data.
Provider makes use of virtual private networks (VPN) between OMNINET branches, sites and seats. In addition, Provider employees, when working remote, can only access the Provider network via a secure SSL VPN connection.
The exchange of data is possible in the customer-specified encrypted format. If personal data is to be returned by Processor towards Controller, the personal data will be encrypted by Processor.
There is no transmission of data to other countries other than the ones mentioned under chapter 18.3.10 ”Processor Agreement SCHEDULE 3 – Sub-Processors”.

d. Segregation of data

In the event that personal data of the customer are processed and collected for different purposes, these personal data are processed separately. Provider strictly separates the testing and production systems.

4. Ensuring integrity

In the event of troubleshooting, data processing (manipulation of data) of customer data does not take place. There is no re-transmission of a database copy from Provider to the customer.

5. Guarantee of availability

a. Availability of data
Personal data is protected against accidental destruction or loss through backup or mirroring of hard drives.
Processor uses a UPS (uninterruptible power supply).
The Processor systems (Servers & Computers) are equipped with up-to-date virus protection programs and firewalls.
A Disaster Recovery Plan is set up tested on regular basis.

b. Order regulations
If necessary, all the measurements for the processing of the requested data are carried out according to predefined instructions.

Database copies are only available to those who need them for the stated purpose. Whenever possible, database copies are used for error analysis and troubleshooting without

personal data. After discontinuation of the support purpose, the database copies are deleted and removed from the systems.
The employees of Processor are regularly trained in data protection topics to ensure they are aware of the consequences of having access to personal data and the proper handling of this data.

6. **Guarantee the load capacity**

   The Provider used infrastructure is dimensioned in terms of storage, access and routing possibilities to ensure that all systems and services are fail-safe in the different load scenarios.
   This is monitored by appropriate monitoring tools. If necessary, the infrastructure will be expanded accordingly. (e.g. review of the monitoring results and events).

7. **Procedures for restoring the availability of personal data after a physical or technical incident**

   In the event of a technical or physical incident that results in the loss of data, the data may be restored based on the periodic backups with a maximum data loss of one day.
   The correct functioning of the backup restore procedure is checked on regular basis using test data.

8. **Procedures for periodic review, evaluation and evaluation of the effectiveness of technical and organizational measures**

   The technical and organizational measures undergo an internal annual review as a whole.
   The audit is carried out by Provider management in collaboration with Provider IT organization.
   As part of this review, the described measures are evaluated against the current available technologies, possible amended laws and updated if necessary.
   If necessary, members from other departments are consulted for evaluation / updates.
   In addition, the compliance of the measures are examined on the basis of random samples.

17.3.10 **Processor Agreement SCHEDULE 3 – Sub-Processors**

As at the date of this Processor Agreement, the following Sub-Processors have been notified by the Processor to the Controller with respect to the Processing:

Provider External Consultants:

a. Working under a ‚freelance‘ contract for the Provider.

OMNINET Business Partners:

b. Working under a ‚partnership‘ agreement for the Contractual Software (OMNIPRIVACY Partner)

Provider Contactual Software internal Support:

a. OMNINET Software-, System- & Projektmanagement GmbH (Germany)
b. OMNINET Holding GmbH (Germany)

SaaS Services data center sub-contractor:

a. PREVIDER Netherlands
   a. https://www.previder.com/
   b. Previder is NEN7510, DigiD Assurance, ISO 9001:2015, 14001:2015 and ISO/IEC 27001:2013 certified.