DATA PROCESSING AGREEMENT

This Data Processing Addendum ("**DPA**"), including its (sub-)appendices, applies to the extent NOVOSERVE processes personal data as a 'data processor' in accordance with Data Protection Legislation, on behalf of CLIENT as a 'data controller' or 'data processor' via the Services as defined by the Terms of Service ("**TOS**"). In the event of a conflict between the terms of this DPA and the TOS, the terms and conditions of this DPA apply, but only to the extent of such conflict.

1. DEFINITIONS

All words herein that are defined in the TOS shall have the meaning assigned to them therein; other words shall have the following meaning:

DEFINITION	**MEANING**
CLIENT Data	Any Personal Data that CLIENT or any End-User transfers to NOVOSERVE for processing via the Services and any Personal Data that CLIENT or any End User derives from the foregoing through its use of the Services.
CLIENT Portal	The online portal available for the CLIENT operated by NOVOSERVE.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Subject	The person to whom the Personal Data relates.
Data Protection Legislation	All laws and regulations relating to the Processing of Personal Data and privacy applicable to NOVOSERVE.

DPA	This agreement, including its accompanying (sub)-appendices.
GDPR	Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016.
Notification Email Address	The email address(es) designated by CLIENT in the CLIENT Portal to receive certain notifications from NOVOSERVE.
Personal Data	Any information relating to an identified or identifiable natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data that is not purely incidental and/or limited in practice,whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1. GENERAL

1.1 The DPA enters into force on the Effective Date and will remain into force as long as the Agreement between CLIENT and NOVOSERVE is in effect and the Services are provided to CLIENT by NOVOSERVE.

1.2 This DPA may be adjusted from time to time to reflect changing circumstances. NOVOSERVE will notify CLIENT of any significant changes. If CLIENT cannot reasonably agree to these changes, CLIENT is entitled to terminate the Agreement within 30 days of notification of the change.

1.3 The applicability of CLIENTS's data processing agreements is expressly rejected.

2. OBJECT OF THIS DATA PROCESSING AGREEMENT

2.1 This DPA governs the Processing of CLIENT Data by NOVOSERVE on behalf of CLIENT. In this context, NOVOSERVE acts as Processor to CLIENT, who can act either as Controller or Processor of the CLIENT Data.
2.2 The CLIENT Data includes the categories of Personal Data that are transferred by CLIENT or End-users to NOVOSERVE via the Services, which may relate to various categories of Data Subjects (e.g. CLIENT's employees, clients, suppliers etc).
2.3 The subject matter of the Processing governed by this DPA is NOVOSERVE's provision of the Services to the CLIENT.
2.4 The purpose of the Processing, governed by this DPA is the provision of the Services by NOVOSERVE to CLIENT. The nature of the Processing may consist of the various actions NOVOSERVE performs in the execution of the Services, such as but not limited to hosting and storing.

3. SCOPE OF NOVOSERVE'S PROCESSING COMPETENCE

3.1 NOVOSERVE will only Process CLIENT Data upon the documented instructions from CLIENT, unless required to do so by laws and/or regulations to which NOVOSERVE is subject; in such a case, NOVOSERVE shall inform CLIENT of that legal requirement before the Processing, unless that law prohibits such information on important grounds of public interest.
3.2 If any instruction, as referred to in Clause 3.1, is deemed by NOVOSERVE to contravene the GDPR or other Data Protection Legislation, NOVOSERVE shall notify CLIENT of this prior to the Processing, unless a statutory law applicable to NOVOSERVE prohibits such notification.

4. SECURITY

4.1 NOVOSERVE will implement the organizational and technological measures to protect the CLIENT Data against unauthorised use or access, loss, destruction, theft or any other unlawful Processing . These measures are described in Appendix 3.1 (the "**Security Measures**"). NOVOSERVE may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.
4.2 CLIENT agrees that the Security Measures provide a level of security appropriate to the risk to the CLIENT Data (taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purposes of the Processing of CLIENT Data as well as the risks to individuals). NOVOSERVE has no obligation to assess CLIENT Data to identify information subject to any specific legal requirements.
4.3 Without prejudice to NOVOSERVE's obligations under Clause 4.1, CLIENT is responsible for its use of the Services and its storage of any copies of CLIENT Data outside NOVOSERVE's or NOVOSERVE's sub-Processors' systems, including:
   a. using the Services and additional security controls to ensure a level of security appropriate to the risk to the CLIENT Data;
   b. securing the account authentication credentials, systems and devices CLIENT uses to access the Services; and
   c. backing up the CLIENT Data as appropriate.

5. PERSONAL DATA BREACH

5.1 NOVOSERVE will inform CLIENT without undue delay after becoming aware of a Personal Data Breach concerning Personal Data Processed by NOVOSERVE via the Notification Email Address, and promptly take reasonable steps to minimize harm and secure CLIENT Data.
5.2 CLIENT is responsible for ensuring that the Notification Email Address remains current and valid.
5.3 NOVOSERVE's notification of a Personal Data Breach will describe:
   a. the nature of the Personal Data Breach including a general description of the CLIENT Data impacted;
   b. the measures, if any, NOVOSERVE has taken, or plans to take, to address the Personal Data Breach and mitigate its potential risk;

c. the measures, if any, NOVOSERVE recommends CLIENT to take to address the Personal Data Breach; and
d. details of a contact point where more information about the Personal Data Breach can be obtained.

5.4 It is up to the Controller (Client or End-User) to assess whether the Personal Data Breach must be reported to a data protection authority or the relevant Data Subjects. Reporting a Personal Data Breach to a data protection authority or Data Subjects always remains the responsibility of the Controller.

6. CONFIDENTIALITY

6.1 NOVOSERVE will treat the CLIENT Data as confidential.
6.2 NOVOSERVE will ensure that access to the CLIENT Data is limited to employees who need access in order to perform the Processing carried out by NOVOSERVE pursuant to the obligations in this DPA and the Agreement.
6.3 NOVOSERVE will ensure that persons authorized to Process CLIENT Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. SUB-PROCESSORS

7.1 Appendix 3.2 includes the sub-Processors that NOVOSERVE engages in the Processing of CLIENT Data.
7.2 CLIENT gives NOVOSERVE permission to engage other sub-Processors for the performance of its obligations under the Agreement.
7.3 NOVOSERVE shall inform CLIENT of any intended changes concerning the addition or replacement of other sub-Processors, thereby giving CLIENT the opportunity to object to such changes on reasonable grounds.
7.4 When engaging any sub-Processor, NOVOSERVE will:
a. ensure via written contract the same data protection obligations as set out in this DPA are imposed on the sub-Processor; and
b. remain fully liable for to the CLIENT for the performance of that sub-Processor's obligations.

8. ASSISTANCE

8.1 If requested by CLIENT, NOVOSERVE will assist CLIENT, insofar as reasonably possible and considered the nature of the Processing and the Services, by appropriate technical and organisational measures for the fulfilment of the CLIENTS's obligation to respond to requests from Data Subjects to exercise the rights set out in chapter III of the GDPR.
8.2 NOVOSERVE will assist CLIENT upon request in ensuring compliance with the obligations pursuant to articles 32 to 36 of the GDPR insofar as reasonably possible and considered the nature of Processing and the Services and the information available to NOVOSERVE.
8.3 NOVOSERVE can charge the reasonable costs it incurs in the context of the assistance provided by NOVOSERVE in the context of this Clause 8 to CLIENT at its then applicable rates.

9. RETURN OR ERASURE OF PERSONAL DATA

9.1 If the Agreement is terminated, NOVOSERVE will erase the CLIENT Data or return it to CLIENT, whichever CLIENT prefers, within 60 days, unless laws and/or regulations applicable to NOVOSERVE require storage of the CLIENT Data.
9.2 NOVOSERVE can charge the reasonable costs it incurs in the context of Clause 9.1 to CLIENT at its then applicable rates.

10. AUDITS

10.1 NOVOSERVE will provide CLIENT with all necessary information to demonstrate compliance with the obligations in this DPA, considering the nature of the Processing and the Services.

10.2 NOVOSERVE will allow for and contribute to audits, including inspections, conducted by CLIENT or third parties assigned by CLIENT to confirm NOVOSERVE's compliance with this DPA. Any such audit will be:

a. requested by CLIENT with at least thirty (30) days' prior notice, and such notice will indicate the reasons for the audit request following which NOVOSERVE and CLIENT will jointly determine the scope of the audit;
b. conducted not more than twice a year unless a data protection authority also requests such audit;
c. conducted at the sole expense of CLIENT.

11. **INTERNATIONAL TRANSFERS**

11.1 NOVOSERVE shall not Process CLIENT Data outside the European Economic Area ("**EEA**"), unless one of the sub-Processors as mentioned in Appendix 3.1 is located outside the EEA. NOVOSERVE will only transfer the CLIENT Data in such cases to countries and/or organisations that provide an adequate level of protection in accordance with the European standards.

11.2 NOVOSERVE will provide CLIENT at its request with more information about international transfers or a copy of the safeguards NOVOSERVE takes where necessary, at the sole discretion of NOVOSERVE.

12. LIABILITY

12.1 As for the Processing of the CLIENT Data, NOVOSERVE is only liable for damages caused by (i) non-compliance with legal obligations in the Data Protection Legislation directly addressed to data processors to the extent NOVOSERVE qualifies as such data processor; or (ii) non-compliance with agreements in this DPA. NOVOSERVE is not responsible or liable for any damages and loss which result from the following of Processing activities of CLIENT, the content of the CLIENT Data or unlawful instructions of CLIENT.

12.2 Any liability for NOVOSERVE for the Processing of CLIENT Data is limited to the total amount that is paid out by the insurance of NOVOSERVE in the specific case for direct damages. If the insurance of NOVOSERVE for any reason does not pay out in the specific situation, the liability is limited to the total amount of fees paid by CLIENT to NOVOSERVE during the preceding three months prior to the month in which the liability causing event took place.

Appendix 3.1 (Technical and Organisational Security Measures)

NOVOSERVE has implemented the following Security Measures:

ENTRY CONTROL
Measures to prevent unauthorized persons from gaining access to data processing systems that process and use personal data:

- Access control system,
  1. NorthC Delft Biometric access control (fingerprint).
  2. NorthC Oude Meer Biometric access control (fingerprint & Card reader).
  3. NovoServe Office (Card reader)
- Door protection (electronic door opener etc.);
- Security and alarm systems;
- Surveillance system, alarm system, video/TV monitor.

The premises of the data center and office are located and secured against unauthorized access with several security measures.

The outdoor areas as well as the entrance areas and corridors of the data center are constantly video-monitored; the images of the motion-sensitive cameras are displayed on the screens of the Network operations control center of NorthC any time they detect motion. Further, all video recordings are stored for 1 month for later evaluation. Only with a written request and approval of the security officer video footage can be seen for the datacenter and the office.

Trained and carefully selected security personnel patrol the location several times at night. Regular access to the building is secured for individual persons via separation systems. Only authorized persons can operate the respective opening mechanisms. For this purpose, personalized chip cards that enable differentiated authorization management for the security areas are issued: access to the data center. Proof of access authorization by means of Biometric access control (access pass +fingerprint) is required both for entering and leaving the secured areas. This allows a complete documentation in this respect.

The individual racks in the datacenter of NOVOSERVE are additionally secured with locks. For suppliers, a delivery point (Loading bay) has been set up in the outermost security area. This is operated by the staff of the datacenter of NorthC. Visitors must be personally met at the entry by authorized persons and accompanied on the premises at all times. If visitors have been reported in advance to security personnel by authorized persons, temporary visitor chip cards with limited access rights will be issued upon presentation of the federal identity card. All visits are logged.

Authorized persons are obligated to carry an identity card on the premises; this must have a photograph.

AVAILABILITY CONTROL
Measures to ensure that personal data is protected against accidental destruction or loss: Backup copies of the data are produced in the following procedures. Description of frequency, medium, retention period, and backup copy storage location:

- Backup procedure (according to contractual agreement)
- Mirroring hard disks, e.g. RAID procedures (according to contractual agreement)
- Antivirus/firewall (according to contractual agreement)
- Emergency plan
- Clarification of existing backups before start of the work

Backups of customer data stored in the data center are either made by the customer itself or by NOVOSERVE according to contractual agreement. If the customer creates the backups on its own, a corresponding dialogue which enables the creation and download of a full backup in a few simple steps is available to the customer in the control panel. If NOVOSERVE is commissioned to create backups according to the contract, a full backup of the stored data is created daily; this is stored on a separate storage system and is available to the customer for download for a period of seven days.

The customer's systems may additionally be mirrored via a RAID procedure, subject to a corresponding contractual agreement.

NOVOSERVE systems have up-to-date virus protection. Subject to the appropriate contractual agreement, the firewall can be configured in a way that ensures that the customer systems can only be accessed from the offices of NOVOSERVE.

The data centers are tier 3 level; It has a UPS (uninterruptible power supply) with N+1 redundancy. The power supply in the event of network failure operates for a period of a minimum of 12 hours.

The data center is equipped with air conditioning; in this respect there is also N+1 redundancy. This ensures a constant room temperature of 24°C (+ 2/-4 ° C). Compliance with these temperature specifications is sensor-monitored. A relative humidity of 55% (+/- 25%) is maintained at the same time.

NorthC Oude Meer
The raw floor load capacity is 15 kN/m2. There is a false floor with a height of 60cm. In this room there is aspiration detection combined with a HI-Fog Water Mist installation.

NorthC Delft
The raw floor load capacity is 11 kN/m2. There is a false floor with a height of 50cm. In this room there is aspiration detection combined with a Water Mist installation.

Additionally, there are fire extinguishers in the server rooms. Protective socket strips guarantee the lowest possible fire risk. flammable packaging material from customers is not allowed in the data room.

Furthermore, the risk of water damage is minimized during the design stages by ensuring that the server rooms were not set up below sanitary facilities. The data rooms are located on the 2th floor in NorthC Delft and on the 3th floor in NorthC Oude Meer.

All fault messages from these systems are reported to the 24/7 control center and forwarded from there to the local authorities and emergency services in accordance with the established emergency plans.

ADMISSION CONTROL
Measures to prevent unauthorized use of data-processing systems:
- State-to-the-art encryption method
- Password procedure (including special characters, minimum length)

Insofar as NOVOSERVE has system sovereignty according to the contract, data is transmitted via SSL encryption. Additionally, VPN connections can be set up and maintained at the customer's request.

NOVOSERVE systems have up-to-date virus protection. Subject to the appropriate contractual agreement, the firewall can be configured in a way that ensures that the customer systems can only be accessed from the offices of NOVOSERVE. Registration on the systems of NOVOSERVE and access to databases are password protected. Passwords are created using a password generator, have at least eight characters and always fulfil at least three of the following four requirements: lowercase letter, uppercase letter, number, special character. Former employees are blocked immediately.

ACCESS CONTROL
Measures to ensure that authorized users of a data processing system can only access the data that is subject to their authorization and that personal data cannot be read, copied, changed or removed during processing, use and after storage without authorization:

Log files can be used to evaluate every access to the systems during the previous six months. As of 2016, access by NOVOSERVE employees is also recorded individually by means of personalized keys.

Video recordings from the data center via motion-sensitive camera systems enable cognizance of system accesses in the data center at all times.

For the destruction of data carriers, cooperation with DIN 32757-certified service providers who certify proper destruction by means of appropriate documentation is in place. For the destruction of personal data on paper a locked box is available, which is picked up for destruction of the contents by appropriately certified service providers when required.

TRANSFER CONTROL
Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers, and that ensure that the locations at which a transfer of personal data by data transmission equipment is intended can be verified and determined:
Description of the equipment used and transmission logs, e.g. identification and authentication, state-of-the-art encryption, automatic callback, etc.

- Encryption;
- Logging;
- Transport safety.

The communication between the client computers of NOVOSERVE and the server takes place via SSL-encrypted data transmission.

INPUT CONTROL
Measures to ensure that it is possible to subsequently ascertain and verify whether and by whom personal data was entered, changed or removed in data-processing systems:

- Logs are kept for at least 6 months by NOVOSERVE;
- Logging and log evaluation systems for authorization assignment.

The log files with which the system accesses are logged are traceable over a period of at least six months. Further, a command history of the past 500 command entries allows transparency even of past system activities.
As of 2016, access by NOVOSERVE employees is also recorded individually by means of personalized keys.

COMMISSION CONTROL

Measures to ensure that personal data processed on commission can only be processed in accordance with the CLIENT's instructions.

Individual customer instructions are filed separately and integrated into the processes. The customer is granted extensive control rights before and during the start of commissioned data processing.

An undertaking to maintain data confidentiality pursuant to GDPR has been obtained from all employees.

SEPARATION CONTROL
Measures to ensure that data collected for various purposes can be processed separately:

- Internal multi-client capability;
- Separation of functions (according to contractual agreement).

Different virtual environments are maintained for individual customers on the physical servers of NOVOSERVE.

Nonetheless, the systems have an internal multi-client capability that ensures at all times that each virtual machine can only access those databases with personal and other data of the respective customer that have been assigned to that machine.

If, for example within the scope of the registration on the system, there is a common database with the access authorization of different customers, multi-tenant-capable software ensures that the information concerning the individual customers is nevertheless separated.

Application software is designed in such a way that there are special access rights to individual, defined databases.

Appendix 3.2 (Sub-Processors)

We currently do not engage any sub-Processors.