NordStellar Data Processing Agreement

Effective from January 27, 2025

This Data Processing Agreement ("**DPA**") is an integral part of the Agreement concluded between the Customer and NordStellar. The main purpose of this DPA is to define how NordStellar processes data on behalf and under the Customer's instructions while providing the Services.

1. DEFINITIONS

1.Unless expressly stated in this DPA, the capitalized terms shall have the meanings indicated below:

Person or **Data Subject**	a natural person whose data is processed.
Personal Data	any information relating to an identifiable Person.
Data Processor	a natural or legal person who processes Personal Data on behalf of and under the instructions of the Data Controller.
Data Controller	a natural or legal person who, in accordance with this DPA, establishes the purposes and means of the processing of Personal Data.
EEA	European Economic Area (all EU Member States and Iceland, Norway and Liechtenstein).
GDPR	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).
Applicable Data Protection Laws	any national or international data protection laws or regulations applicable to the Data Controller and/or Data Processor, for the duration of this DPA. The Applicable Data Protection Laws shall include the GDPR.
Processing	any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sub-Processor	a natural or legal person (including any third party and any Data Processor's Affiliate but excluding employees of the Processor or any of its sub-contractors and consultants) appointed by the Data Processor to Process Personal Data on behalf of the Data Controller, in accordance with its instructions, the terms of this DPA.
Standard Contractual Clauses / SCCs	the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
Agreement	means the Master Service Agreement concluded between NordStellar and Customer.

2.Terms and expressions used in this DPA and not defined herein shall have the meaning assigned to them in the Agreement.

2. GENERAL PROVISIONS

1.**Scope.** This DPA applies to the Processing of Personal Data as specified in Annex I to this DPA. Annexes form an integral part of this DPA.

2.When processing Personal Data under this DPA, the Data Processor shall comply with its provisions, as well as all Applicable Data Protection Laws and recommendations of the competent supervisory authorities.

3.**Interpretation.** Where this DPA uses the terms defined in the GDPR, those terms shall have the same meaning as in that regulation. This DPA shall be read and interpreted in the light of the provisions of the GDPR, and shall not be interpreted in a way that runs counter to the rights and obligations

provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

4. **Hierarchy.** In the event of a contradiction between this DPA and the Agreement, this DPA shall prevail.

3. OBLIGATIONS OF THE PARTIES

1. The Data Controller has the right and obligation to make decisions about the purposes and means of the Processing of Personal Data.

2. The Data Processor shall comply with its obligations under this DPA and Applicable Data Protection Laws and shall not, by any act or omission, cause the Data Controller to incur any liability under any of the Applicable Data Protection Laws or other laws.

3. **Purpose limitation.** The Data Processor warrants and undertakes to process the Data Controller's Personal Data only for the limited and specified purposes set out in the Agreement and/or as otherwise lawfully instructed by the Data Controller in writing and mutually agreed by the Parties, except where otherwise required by the Data Protection Laws. The Data Processor will not process the Data Controller's Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Laws.

4. **Instructions.** The Data Controller's initial instructions to the Data Processor are set forth in this DPA and its Annex I. All the instructions provided are comprehensive and reflect the Data Controller's will.

5. The Data Processor shall not evaluate any instructions of the Data Controller, which shall be held responsible and liable for any given instructions, to be fully lawful and compliant with the applicable Data Protection Laws. If in the Data Processor`s reasonable opinion, an instruction undoubtedly infringes the applicable Data Protection Laws, the Data Processor shall notify the Data Controller. The Data Processor is not responsible for compliance with any Data Protection Laws applicable to the Data Controller or its industry that are not generally applicable to the Data Processor.

6. The Data Processor shall:

    1. only carry out Processing of Personal Data on the Data Controller's written instructions;

    2. inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or other Applicable Data Protection Laws and request that the Data Controller withdraw, amend, or confirm the relevant instruction. Pending the decision on the withdrawal, amendment, or confirmation of the relevant instruction, the Data Processor shall be entitled to suspend the implementation of the relevant instruction.

7. The Data Controller shall ensure that its instruction to the Data Processor comply with all laws, rules, and regulations applicable to Personal Data, and that the Processing of Personal Data per Data Controller's instructions will not cause Data Processor to be in breach of Applicable Data Protection Law. The Data Controller is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to the Data Processor by or on behalf of the Data Controller; (ii) how the Data Controller acquired any such Personal Data; and (iii) the instructions the Data Controller provides to the Data Processor regarding the Processing of Personal Data. The Data Controller shall not provide or make available to the Data Processor any Personal Data in violation of the Agreement, this DPA and shall indemnify the Data Processor from all claims and losses in connection therewith.

8. In particular but without prejudice to the generality of the foregoing, the Data Controller acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of the Data Controller's Personal Data and the means by which it acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including any necessary notifications to Data Subjects, consents, and authorizations that are needed for the Data Controller's use of the Data Processor's Services; (iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Data Processor for processing in accordance with the provisions of the Agreement (including this DPA). The Data Controller shall also inform the Data Processor without undue delay if the Data Controller is not able to comply with its responsibilities under this Section.

9. **Duration.** Processing by the Data Processor shall only take place for the duration specified in Annex I of this DPA.

10. **Data disclosure.** The Data Processor shall ensure that all persons authorized to Process Personal Data are made aware of the confidential nature of the Personal Data and have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality.

11. In case any Person, competent authority or any other third-party requests information from the Data Processor about the Personal Data processed under this DPA, the Data Processor shall inform the Data Controller of such request. The Data Processor may in no way act on behalf of the Data Controller, or as its representatives, and may not transfer or otherwise disclose any Personal Data or other information related to the Processing to third parties without prior instructions from the Data Controller. If the Data Processor is required to disclose Personal Data processed on behalf of the Data Controller in accordance with the Applicable Data Protection Laws or other legal acts, the Data Processor informs the Data Controller.

12. **Sensitive data.** If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a Person, data concerning health or a Person's sex life or sexual orientation, or data relating to criminal convictions and offenses ("**sensitive data**"), the Data Processor shall apply specific restrictions and/or additional safeguards.

4. USE OF SUB-PROCESSORS

1. The Data Processor has the Data Controller's general authorisation for the engagement of Sub-Processors. The Data Processor maintains a list of Sub-Processors and, upon receiving a written request from the Data Controller, provides the Data Controller with such a list.

2. The Data Processor shall: (i) ensure that any Sub-Processor is contractually bound in writing to provide at least the same level of protection as is required by this DPA and complies with the Data Protection Laws; (ii) be fully responsible and liable to the Data Controller for acts and omissions of any Sub-Processor as if they were Data Processor's own act or omission. If required to do so by applicable Data Protection Laws, in case of a new Sub-Processor: (i) the Data Processor will inform the Data Controller thereof; and (ii) the Data Processor shall enable the Data Controller to object, by way of providing to Data Processor with a reasoned, specific and written objection within thirty (30) days following the notification of the changes in the Sub-Processors. If the Data Controller does not object to a new Sub-Processor's engagement within the term of notice issuance from the Data Processor, that new Sub-Processor shall be deemed acceptable.

3. If the Data Controller objects to the engagement of a new Sub-Processor, the Data Processor shall have the right resolve the objection through one of the following options which is selected at the Data Processor's sole discretion:

    1. The Data Processor cancels its plans to use the Sub-Processor with regard to Data Controller's Personal Data;
    2. The Data Processor will take the corrective measures requested by the Data Controller in its objection which would resolve the Data Controller's objection and proceed to use the Sub-Processor with regard to Data Controller's Personal Data;
    3. The Data Processor may cease to provide, or Data Controller may agree not to use (temporarily or permanently), the particular aspect of the Service that would involve the use of such Sub-Processor with regard to Data Controller's Personal Data;
    4. The Data Processor provides the Data Controller with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Service. If the Data Processor, in its sole discretion, cannot provide any such alternative(s) or if the Data Controller does not agree to any such alternative(s), if provided, the Data Processor and the Data Controller, within 30 (thirty) calendar days of being provided an alternative, may terminate the affected portion(s) of the Agreement with prior written notice. Termination will not relieve the Data Controller of any Fees or charges owed to the Data Processor for Services provided up to the effective date of the termination under the Agreement.

4. Where the Data Processor engages a Sub-Processor for carrying out specific Processing activities (on behalf of the Data Controller), it shall do so by way of a contract which imposes on the Sub-Processor, in substance, consistent data protection obligations as the ones imposed on the Data Processor in accordance with this DPA. The Data Processor shall ensure that the Sub-Processor complies with the obligations to which the Data Processor is subject pursuant to this DPA and the GDPR.

5. If Personal Data is transferred to a Sub-Processor in a third country that does not ensure an adequate level of protection according to the European Commission, the Data Processor shall ensure the transferred data are processed with the same GDPR transfer guarantees as agreed with the Data Controller. The Data Processor shall also perform a case-by-case assessment if supplementary

measures are required in cases of onward transfers to third countries to bring the level of protection of the transferred data up to the EU standard of essential equivalence.

6. The Data Processor shall remain fully responsible to the Data Controller for the performance of the Sub-Processor's obligations in accordance with its contract with the Data Processor. The Data Processor shall notify the Controller of any failure by the Sub-Processor to fulfill its contractual obligations.

5. TRANSFERS TO THIRD COUNTRIES

1. The Data Controller acknowledges and agrees that the Data Processor may transfer and Process Data Controller's Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement. The Data Processor may transfer Personal Data to third countries (including those outside the EEA without an adequacy decision from the European Commission) to Affiliates, professional advisors, or its Sub-Processors. The Data Processor will ensure that such transfers are made in compliance with the Applicable Data proception Law and this DPA.

2. Any transfer of the Data Controller's Personal Data made subject to this DPA from member states of the EU, the EEA to any country that does not ensure the adequate level of protection according to the European Commission, shall be undertaken through the Standard Contractual Clauses in connection to which the Parties agree to the following:

    1. Controller to Processor / Processor to Processor transfers, in relation to Personal Data that is protected by the GDPR and processed in accordance with this DPA, the SCCs shall apply, completed as follows:

        1. Module Two or Module Three will apply (as applicable);
        2. In Clause 7, the optional docking clause will apply;
        3. In Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Clause 4.3 of this DPA;
        4. In Clause 11, the optional language will not apply;
        5. In Clause 17, Option 1 will apply, and the SCCs will be governed by the Netherlands law;
        6. In Clause 18(b), disputes shall be resolved before the courts of Netherlands;
        7. Annex I of the SCCs shall be deemed completed with information set out in Annex I to this DPA; and
        8. Subject to Clause 6.3 of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in Annex II to this DPA.

3. The Standard Contractual Clauses shall be applicable to the relationships between the Parties, to the extent relevant and to the extent objective legal and factual grounds exist for such application. If and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement and this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict. Standard Contractual Clauses shall be considered to constitute an integral part of this DPA.

4. The Data Processor will follow Applicable Data Protection Law requirements concerning the completion of a data transfer impact assessment.

6. CONFIDENTIALITY AND SECURITY

6.1. The Data Processor shall ensure that access to the Personal Data is limited to those Data Processor's employees or authorized third persons who need access to the Personal Data to meet the Data Processor's obligations under the Agreement and that all such employees and authorized third persons are informed of the confidential nature of Personal Data and have undertaken to ensure the confidentiality thereof.

6.2. In order to assist the Data Controller in complying with its legal obligations, the Data Processor shall implement appropriate technical and organizational security measures to protect the Personal Data processed on behalf of the Data Controller and comply with all data security policies and instructions specified by the Data Controller. Those measures must ensure an adequate level of security and may include the following:

6.2.1. pseudonymisation and encryption of Personal Data;

6.2.2. ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and Services;

6.2.3. ensuring the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident;

6.2.4. processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing.

6.3. The Data Processor shall at least implement the technical and organizational measures specified in Annex II to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data ("**Personal Data Breach**"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

6.4. In any case, the Data Processor shall ensure that such technical and organizational measures: (i) are no less rigorous than those maintained by the Data Processor in respect of the Data Processor's own information and data (including Personal Data) of a similar nature; (ii) comply with information security requirements; (iii) comply with the best information security practices common to the reputable companies acting in the same industry as the Data Processor.

7. ASSISTANCE AND COOPERATION

7.1. The Data Processor shall provide to the Data Controller all reasonably necessary assistance and cooperation in relation to: (i) implementation of technical and organizational measures necessary to protect the Personal Data (Clause 6); (ii) notifying Personal Data Breaches to the competent supervisory authority (Clause 9); (iii) any claim and/or exercise or purported exercise of rights by a Data Subject under the Applicable Data Protection Laws; (iv) advising Data Subjects when there has been a Personal Data Breach; (v) any investigation or enforcement activity by the competent supervisory authority, relating to, connected with or arising out of the Processing of Personal Data; (vi) any internal data protection impact assessment or prior consultations; (vii) ensuring that Personal Data is accurate and up to date, by informing the Data Controller without delay if the Data Processor becomes aware that the Personal Data it is processing is inaccurate or has become outdated.

7.2. The Data Processor also shall notify the Data Controller immediately, if it is contacted or approached regarding the Processing or regarding issues connected with, or arising out of such, regarding:

7.2.1. any Data Subject access request;

7.2.2. any other request from a Data Subject;

7.2.3. any claim for damages under the Applicable Data Protection Laws; and/or

7.2.4. any investigation or enforcement activity by the competent supervisory authority.

8. DOCUMENTATION AND COMPLIANCE. AUDIT AND INSPECTION

8.1. The Parties shall be able to demonstrate compliance with this DPA.

8.2. The Data Processor shall deal promptly and adequately with inquiries from the Data Controller about the Processing of data in accordance with this DPA.

8.3. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from the GDPR. At the Data Controller's request, the Data Processor shall also permit and contribute to audits of the Processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Data Controller may take into account relevant certifications held by the Data Processor.

8.4. The Data Controller may choose to request for an audit at its expense. Following a receipt by the Data Processor of a request for an audit, the Parties will discuss and agree in advance on:

8.4.1. the identity of an independent and suitably qualified third-party auditor to conduct the audit;

8.4.2. the reasonable start date and duration (not to exceed two weeks in respect if any premise audits) of any such audit;

8.4.3. the scope, process and normative framework of the audit, including (i) the data processing outcomes, information and control requirements to be in scope of the audit evidence requirements; and (ii) the nature and process for satisfactory audit evidence; and

8.4.4. the security and confidentiality controls applicable to any such audit. All audits must be conducted in accordance with recognized international auditing standards.

8.5. Nothing in this DPA will require the Data Processor to provide Personal Data of other Data Processor's customers or access to any Data Processor's systems or facilities that are not involved in the provision of Services to Controller under the Agreement.

9. PERSONAL DATA BREACHES

9.1. **Data breach concerning Personal Data processed by the Data Controller**. In the event of a Personal Data Breach concerning data processed by the Data Controller, the Data Processor shall assist the Data Controller:

9.1.1. report the breach to the Data Controller without undue delay, after becoming surely aware of the Personal Data Breach;

9.1.2. make reasonable efforts to assist the Data Controller in fulfilling its obligation under applicable Data Protection Laws to notify a relevant supervisory authority and/or data subjects about such Personal Data Breach.

9.1.3. For the avoidance of doubt, the Data Processor will not notify and/or disclose any information relating to the Personal Data Breach to any third party, including but not limited to data subjects and supervisory authority, unless required to do so by Data Protection Laws.

10. TERM AND TERMINATION

The provisions of this DPA shall apply to the extent that the Data Processor processes the Personal Data on behalf of the Data Controller in accordance with the Agreement, unless the Parties terminate the Agreement and/or this DPA earlier on the grounds provided therein.

11. ERASURE AND RETURN OF PERSONAL DATA

Following termination of the Agreement (unless the Data Controller requests earlier), the Data Processor shall, under the request and choice of the Data Controller: (i) delete all Personal Data processed on behalf of the Data Controller and certify to the Data Controller that it has done so; or (ii) return all Personal Data to the Data Controller and delete existing copies, unless the EU or Member State law requires storage of that Personal Data. Until the Personal Data is deleted or returned, the Data Processor shall continue to ensure compliance with this DPA.

12. LIABILITY

NordStellar's liability, taken together in the aggregate, arising out of or related to this DPA, whether contractual, tort or under any other theory of liability, shall be subject to the limitations and exclusions set out in the Agreement. Liability of NordStellar shall mean the aggregate liability of NordStellar under the Agreement and this DPA together.

13. NOTICES

All notices from one Party to the other relating to this DPA shall be delivered following the provisions of the Agreement.

14. APPLICABLE LAW AND JURISDICTION

This DPA shall be governed and any disputes or claims arising from this DPA shall be settled according to the provisions of the Agreement.

ANNEX I

DESCRIPTION AND INSTRUCTIONS FOR DATA PROCESSING/TRANSFER

A. LIST OF PARTIES

Data Exporter	**Data Importer**
Customer	NordStellar
Activities relevant to the data transferred: **As described in Section B below.**	Activities relevant to the data transferred: As described in Section B below.
Role: **Controller**	Role: Processor

B. DESCRIPTION OF PROCESSING / TRANSFER

Purposes of Processing	**Provision of Services under the Agreement.**
Categories of Personal Data	**API Queries and/or Monitored Assets** **Customer Data categories:** Monitored Assets: ● Phone number; ● Credit card number; ● Any additional data provided by the Customer to ascertain their involvement in the data leak, including keywords, domain names, email addresses and other data points or information that Customer or Authorized User provides to the NordStellar (through API/Platform or any other mean) for monitoring and alerting of potential breach; ● the fact that the data listed above were leaked / not leaked. API Queries: As keywords, email addresses or other data point or information that Customer or Authorized User submits via API or otherwise identify as query terminology or criteria relevant to Data Subjects to detect potential breach of data security. Data retrieved from Data Importer Sub-Processor databases based on requests formulated by the Data Exporter: Credential lists containing simple combinations of emails or usernames and passwords. Data retrieved from public registries and other public sources during the provision of Services related to Monitored Assets, to the extent such data involves Personal Data: Contact details and other Personal Data related to domain name registrations.

Sensitive Personal Data (*Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses*), if applicable	N/A
Categories of Data Subjects	Customer's employees (current and former) and / or Customer's clients; Potentially, third parties.
Frequency of Processing / Transfer	Continuous
Nature of Processing	NordStellar will process Customer's Personal Data for the purposes of providing the Services to Customer in accordance with the Agreement.
Duration of Processing	Term of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

ANNEX II

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY THE DATA PROCESSOR

SECURITY

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

Data Processor shall implement at least the following minimal technical and organisational security measures and ensure that they are properly adhered to (this is not an exhaustive list of applicable security measures).

MANAGEMENT OF SECURITY

Security policy. Data Processor shall have a properly documented Personal Data security policy, which may be a part of information security policy. This policy shall be regularly reviewed and revised if necessary.

Roles and responsibilities. Roles and responsibilities related to the Processing of Personal Data shall be clearly defined and allocated in accordance with the security policy. During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures shall be clearly defined.

Access rights management. Specific access control rights shall be allocated to each role (involved in the Processing of Personal Data) following the need-to-know principle.

Resource management. Data Processor shall keep a registry of all currently operated data processing information systems and other IT resources and assets (devices, hardware, software, networks) which shall be regularly renewed.

Change management. Data Processor shall make sure that all changes to the Service are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place. Software development shall be performed in a special environment that is not connected to the Service used for the Processing of Personal Data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of Personal Data used in testing.

Data Processors. Formal guidelines and procedures covering the selection of data processors as well as the processing of personal data by data processors contracted by the Data Processor should be defined and documented. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the Data Processor's security policy.

PERSONAL DATA SECURITY BREACH MANAGEMENT AND BUSINESS CONTINUITY

Personal data security breaches. Data Processor shall have an incident response plan with detailed procedures to ensure effective and orderly response to incidents pertaining to personal data.

Business continuity. Data Processor shall establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the Service processing personal data (in the event of an incident/Personal Data Breach).

HUMAN RESOURCES

Training. Data Processor shall ensure that all employees (including temporary workers, contractors etc.) are adequately informed about the security controls of the Service that relate to their everyday work. Employees involved in the processing of personal data shall also be properly informed about relevant data protection requirements and legal obligations through regular awareness courses.

TECHNICAL SECURITY MEASURES

Access control and Authorized User authentication. Data Processor shall implement an access control system applicable to all Authorized Users accessing the Service. The system shall allow creating, approving, reviewing and deleting Authorized User accounts. The use of common Authorized User accounts should be avoided. In cases where this is necessary, it should be ensured that all Authorized Users of the common account have the same roles and responsibilities. An authentication mechanism shall be implemented, allowing access to the Service (based on the access control policy and system). As a

minimum a username/password combination shall be used. Passwords shall respect a certain (configurable) level of complexity.

Logging and monitoring. Log files shall be activated for each system/application used for the processing of personal data. They shall include all types of access to data (view, modification, deletion). Log files shall be time stamped and adequately protected against tampering and unauthorized access. Clocks shall be synchronized to a single reference time source.

Security of data at rest. Database and applications servers shall be configured to run using a separate account, with minimum OS privileges to function correctly. Database and applications servers should only process the personal data that are actually needed to process in order to achieve its processing purposes.

Workstation security. Authorized Users shall not be able to deactivate or bypass security settings. Anti-virus applications and detection signatures shall be configured on a weekly basis. Authorized Users shall not have privileges to install or deactivate unauthorized software applications. The system shall have session time-outs when the Authorized User has not been active for a certain time period. Critical security updates released by the operating system developer shall be installed regularly.

Network and communications security. Whenever access is performed through the Internet, communication shall be encrypted through cryptographic protocols (TLS/SSL).

Back-ups. Backup and data restore procedures shall be defined, documented and clearly linked to roles and responsibilities. Backups shall be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data. Execution of backups should be monitored to ensure completeness. Full backups should be carried out regularly.

Mobile and portable devices. Mobile and portable device management procedures shall be defined and documented establishing clear rules for their proper use. Mobile devices that are allowed to access the information system shall be pre-registered and pre-authorized. Mobile devices shall be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.

Application lifecycle security. During the development lifecycle best practices, state of the art and well acknowledged secure development practices, frameworks or standards shall be followed. Specific security requirements shall be defined during the early stages of the development lifecycle. Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) shall be adopted in analogy to the security requirements. Secure coding standards and practices shall be followed.

Deletion and disposal of data. Software-based overwriting shall be performed on all media prior to their disposal. In cases where this is not possible physical destruction shall be performed. Shredding of paper and portable media used to store personal data shall be carried out after their storage period expires.

Physical security. The physical perimeter of the Service infrastructure shall not be accessible by non-authorized personnel.

When assessing the appropriate level of security, the Data Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

ANNEX III

CCPA DATA PROTECTION ADDENDUM

1. This CCPA Data Protection Addendum ("**Addendum**") reflects the requirements of the CCPA and is in effect for as long as NordStellar maintains Personal Information (as defined in and to the extent protected by the CCPA) provided by the Customer or which is collected on behalf of the Customer by NordStellar ("**Personal Information**").

2. This Addendum prevails over any conflicting terms of the Agreement or DPA but does not otherwise modify the Agreement or DPA.

3. The following terms used but not defined in the DPA or this Addendum, such as "**Business**", "**Service Provider**", "**Business purpose**", "**Consumer**" and "**Third party**" will have the same meaning as set forth in the CCPA.

4. **Scope and Applicability of this Addendum**.

1. This Addendum shall only apply and bind the Parties if and to the extent the Customer is the Business and the Customer appoints NordStellar as the Service Provider to process the Personal Information on behalf of the Customer.

2. This Addendum applies to the collection, retention, use, and disclosure of the Personal Information to provide the Services to the Customer pursuant to the Agreement or to perform a Business purpose.

3. NordStellar's collection, retention, use, or disclosure of Personal Information for its own purposes independent of providing the Services specified in the Agreement are outside the scope of this Addendum.

5. **Restrictions on Processing**

1. NordStellar is prohibited from retaining, using, selling or disclosing the Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Agreement for the Customer, as set out in this Addendum, or as otherwise permitted by the CCPA.

6. **Consumer Rights**

1. If NordStellar, directly or indirectly, receives a request submitted by a Consumer to exercise a right they have under the CCPA in relation to that Consumer's Personal Information, it will provide a copy of the request to the Customer.

2. NordStellar shall provide reasonable assistance to the Customer in facilitating compliance with Consumers rights requests.

3. Upon direction by the Customer and within a commercially reasonable amount of time, NordStellar shall delete the Personal Information.

7. **No Sale of Personal Information**

1. The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement, the DPA, or this Addendum.