DATA PROCESSING ADDENDUM

This DPA is entered into between the Customer and Active Navigation, Inc., a Delaware corporation, d/b/a ActiveNav (**ActiveNav**), and is incorporated into and governed by the terms of the Subscription Services Agreement between the parties.

DEFINITIONS.

Any capitalized term not defined in this DPA will have the meaning given to it in the Agreement (defined below).

- **Affiliate** *means* any entity that directly or indirectly controls, is controlled by, or is under common control of a party. 'Control' for purposes of this definition *means* direct or indirect ownership or control of more than 50% of the voting interests of a party.
- **Agreement** *means* the Subscription Services Agreement between the Customer and ActiveNav for the provision of the Services.
- **CCPA** *means* the California Consumer Privacy Act of 2018, along with its regulations, and as amended.
- **Controller** *means* the Customer, the entity which determines the purposes and means of the process of Personal Data.
- **Customer Data** *means* data, which may include personal data and the categories of data submitted, stored, sent, or received via the Services by Customer, its Affiliates, or end users.
- **Data Protection Laws** *means* (a) the GDPR and any national law supplementing the GDPR (such as, in the UK, the Data Protection Act 2018) or any successor laws arising out of the withdrawal of a member state from the European Union, and (b) any data protection or privacy laws, regulations, regulatory requirements, guidance and codes of practice applicable to the processing of Personal Data under the Agreement, including but not limited to CCPA.
- **Data Subject** *means* (i) the identified or identifiable person to whom Personal Data relates; or (ii) a "Consumer" as the term is defined in the CCPA.
- **DPA** *means* this data processing addendum and its schedules (together).
- **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.
- **Model Contract Clauses** *means* the standard contractual clauses for personal data transfer from controllers to processors c2010-593 - Decision 2010/87EU set out in **Schedule 4** of this DPA.
- **Personal Data** *means* any information relating to: (i) an identified or identifiable natural person and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws), which is provided as Customer Data.
- **Processor** *means* ActiveNav, the entity which Processes Personal Data on behalf of Controller, including as applicable any "Service Provider" as that term is defined by the CCPA.

- **Sub-processors** *mean* any person or entity engaged by ActiveNav or an Affiliate to process Personal Data in the provision of the Services to Customer.

- **Supervisory Authority** *means* a governmental or government-chartered regulatory body having binding legal authority over Customer.

- **Services** *means* the web subscription services provided by ActiveNav.

1. PURPOSE.

a. ActiveNav has agreed to provide the Services to the Customer in accordance with the terms of the Agreement. In providing the Services, ActiveNav will process Customer Data on behalf of the Customer. Customer Data may include Personal Data. ActiveNav will process and protect such Personal Data in accordance with the terms of this DPA and the Data Protection Laws.

b. With respect to Customer Data under this DPA, the parties agree that Customer is the 'data controller' and ActiveNav is the 'data processor'. Customer will comply with its obligations as a controller and ActiveNav will comply with its obligations as a processor under the DPA.

c. Where a Customer Affiliate or a Customer client is the controller with respect to certain Customer Data, Customer represents and warrants to ActiveNav that it is authorized to instruct ActiveNav and otherwise act on behalf of such Customer Affiliate or Customer client in relation to the Customer Data in accordance with the Agreement and this DPA.

2. SCOPE.

In providing the Services to the Customer pursuant to the terms of the Agreement, ActiveNav will treat Personal Data as confidential and only process Personal Data on behalf of the Customer, and only to the extent necessary to provide Services and in accordance with the Customer's instructions as documented in the Agreement and this DPA.

3. ACTIVENAV OBLIGATIONS.

d. ActiveNav may collect, process, or use Personal Data only in accordance with the scope of the Agreement, this DPA, and Customer's instructions. This DPA is Customer's complete and final documented instruction to ActiveNav in relation to Personal Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between ActiveNav and Customer, including agreement on any additional fees payable by Customer to ActiveNav for carrying out such instructions.

e. ActiveNav will ensure that all employees, agents, officers, and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by terms materially no less restrictive than the terms of this DPA.

f. ActiveNav must maintain appropriate managerial, operational, and technical safeguards designed to preserve the integrity and security of Customer Data while in its possession and control hereunder, while taking into account the state of the art, 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.

g. ActiveNav must maintain appropriate measures to ensure a level of security appropriate to the risk, as further set forth in **Schedule 2**.

h. Customer agrees that, in the course of providing the Services to the Customer, it may be necessary for ActiveNav to access the Personal Data to respond to any technical problems, Customer queries, security monitoring, and to ensure the proper working of the Services. All such access by ActiveNav will be limited to those purposes and performed by authorized personnel.

i. Where Personal Data relating to an EU Data Subject is transferred outside of the European Economic Area (**EEA**), it will be processed in accordance with the provisions of the Model Contractual Clauses, unless the processing takes place: (i) in a third country or territory recognized by the EU Commission to have an adequate level of protection; or (ii) by an organization located in a country which has other legally recognized appropriate safeguards in place, such as the Binding Corporate Rules.

j. ActiveNav will reasonably assist the Customer in meeting its obligation to carry out Data Protection Impact Assessments (**DPIA**), taking into account the nature of processing and the information available to ActiveNav.

k. Customer and ActiveNav and, where applicable, their representatives, will cooperate, upon request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

l. ActiveNav may not (i) sell Personal Data; (ii) retain, use or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement. ActiveNav understands these restrictions.

4. CUSTOMER OBLIGATIONS.

m. Customer represents and warrants, in its use of the Services, that it will comply with the terms of the Agreement, this DPA, and the Data Protection Laws. All Affiliates of Customer who use the Services will comply with the obligations of the Customer set out in this DPA.

n. Customer represents and warrants that, as having sole responsibility for the Data quality, legality, and accuracy, has obtained any and all necessary permissions and authorizations necessary to permit ActiveNav, its Affiliates, and Sub-processors, to execute their rights or perform their obligations under this DPA.

o. Customer represents and warrants that: (i) its instructions comply with Data Protection Laws; and (ii) some instructions from the Customer, including assisting with audits, inspections, or DPIAs by ActiveNav, beyond the reasonable assistance ActiveNav generally provides to its customers during an audit, inspection, or DPIA, may result in additional fees. ActiveNav will notify the Customer in advance of its fees for providing such assistance in advance.

p. Customer must inform ActiveNav of any notice, inquiry (including any notice, investigation, complaint, or request) relating to Processor's processing of Personal Data and provide Processor with a copy thereof within 48 hours of receipt. Notices should be emailed to: privacy@activenav.com and if in hard copy to:

F.A.O: Operations
ActiveNav Inc.
P.O. Box 3423
Reston, VA 20195

5. NOTIFICATION OF SECURITY BREACH.

q. ActiveNav will notify the Customer without undue delay after becoming aware of (and in any event within 72 hours of discovering) any confirmed accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to Customer's Personal Data (**Data Breach**).

r. ActiveNav will take all commercially reasonable measures to secure the Personal Data, to eliminate the Data Breach, and to assist the Customer in meeting the Customer's obligations under applicable law. In the event of a Data Breach, ActiveNav's System Administration Team and Security Team will perform a risk-based assessment of the situation and develop appropriate strategies in accordance with ActiveNav incident response procedures, which include contacting the Customer and to contact Customer's primary (technical or business) point of contact or Security Operation Center (**SOC**) to brief them on the situation and provide resolution status updates.

6. AUDIT.

s. ActiveNav will make available to the Customer all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

t. Any audit conducted under this DPA will consist of examination of the most recent reports, certificates, and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Customer, the Customer may conduct a more extensive audit which will be: (i) at the Customer's expense; (ii) limited in scope to matters specific to the Customer and agreed in advance; (iii) carried out during business hours and upon reasonable notice which must be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with ActiveNav's day-to-day business. Any such audit must be conducted remotely, except Customer and/or its Supervisory Authority may conduct on on-site audit at ActiveNav's premises if so, required by the Data Protection Laws. In no event will any audit of a Sub-processor, beyond a review of reports, certifications and documentation made available by the Sub-processor, be permitted without the Sub-processor's consent. This clause does not modify or limit the rights of audit of the Customer, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

7. DATA SUBJECTS.

u. ActiveNav must, to the extent legally permitted, promptly notify Customer if ActiveNav receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, object to the processing (**Data Subject Request**).

v. Considering the nature of the processing, ActiveNav must assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under the Data Protection Laws.

w. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, ActiveNav must upon Customer's request, and to the extent possible, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent ActiveNav is legally permitted to do so and the response to such Data Subject Request is required under data protection laws. To the extent legally permitted, Customer must be responsible for any costs arising from ActiveNav's provision of such assistance.

8. SUB-PROCESSORS.

x. The Customer agrees that: (i) Affiliates of ActiveNav may be used as Sub-processors; and (ii) ActiveNav and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services. The current list of Sub-processors is on **Schedule 3**.

y. All Sub-processors who process Personal Data in the provision of the Services to the Customer will comply with the obligations of ActiveNav set out in this DPA.

z. Where Sub-processors are located outside of the EEA, ActiveNav confirms that such Sub-processors: (i) are located in a third country or territory recognized by the EU Commission to have an adequate level of protection; (ii) have entered into the Model Contract Clauses with ActiveNav; or (iii) have other legally recognised appropriate safeguards in place, such as the Binding Corporate Rules.

aa. During the term of this DPA, ActiveNav will provide the Customer with prior notification, via email, of any changes to the list of Sub-processors who may process Personal Data before authorizing any new or replacement Sub-processors to process Personal Data in connection with the provision of the Services.

bb. The Customer may object to the use of a new or replacement Sub-processor, by notifying ActiveNav promptly in writing within 10 business days after receipt of ActiveNav's notice. If the Customer objects to a new or replacement Sub-processor, and that objection is not unreasonable, the Customer may terminate the Agreement or applicable order with respect to those Services which cannot be provided by ActiveNav without the use of the new or replacement Sub-processor. ActiveNav will refund the Customer any prepaid and unused fees covering the remainder of the term of the applicable order following the effective date of termination with respect to such terminated Services.

9. INSTRUCTIONS.

a. For the purposes of Clause 5(a) of the Model Contract Clauses, the following are deemed to be instructions by the Customer to process Personal Data: (i) the Agreement and applicable orders; and (ii) commands and actions initiated by the Customer users in the Services.

b. Pursuant to Clause 5(h) of the Model Contract Clauses, the Customer agrees that ActiveNav may engage new Sub-processors as described in Sections 8.d and 8.e. of this DPA.

c. The parties further agree that the copies of the Sub-processor agreements that must be provided by ActiveNav to the Customer pursuant to Clause 5(j) of the Model Contract Clauses may have all commercial information, or clauses unrelated to the Model Contract Clauses or their equivalent, removed by ActiveNav beforehand; and, that such copies will be provided by ActiveNav only upon the written request of the Customer.

d. The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Model Contract Clauses must be carried out in accordance with the specifications in Section 6 of this DPA.

e. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Model Contract Clauses must be provided by ActiveNav only upon the Customer's request.

10.LIABILITY.

f. The parties agree that ActiveNav will be liable for any breaches of this DPA caused by the acts and omissions of its Sub-processors to the same extent ActiveNav would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

g. The parties agree that the Customer will be liable for any breaches of this DPA caused by the acts and omissions of its Affiliates and users as if such acts and omissions had been committed by Customer itself.

11.TERM AND TERMINATION.

h. This DPA will automatically terminate upon the termination of the Agreement.

i. ActiveNav will, upon written request: (i) make the Services available to Customer for the return Customer Data to the Customer at the expiration of the order within the time periods set out in the Agreement; (ii) securely delete all Customer Data after such time period unless applicable law with respect to ActiveNav prevent destruction of the Customer Data; and (iii) provide a certification of deletion of Customer Data.

j. Where any Customer Data is retained for such reasons, the Customer Data must be treated as Confidential Information and will no longer be actively processed.

12.GENERAL.

k. This DPA sets out the entire understanding of the parties, and supersedes all prior and contemporaneous agreements and understandings, with regards to the subject matter. No modification or waiver of any term in this DPA is effective unless both parties sign it.

l. Should a provision of this DPA be invalid or become invalid, then the legal effect of the other provisions will be unaffected. A valid provision is deemed to have been agreed upon, which comes closest to what the parties intended commercially and will replace the invalid provision. The same will apply to any omissions.

m. To the extent of any conflict or inconsistency between the terms of this DPA, the Model Contract Clauses, and the Agreement, the following order of precedent applies: The Agreement, including without limitation the disclaimer of damages and limitation of liability in the Agreement, the Model Contract Clauses, and this DPA. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

n. Customer may send any questions or concerns regarding this DPA to: privacy@activenav.com

Schedules Attached

Schedule 1 - Categories of Data

Schedule 2 - Technical and Organizational Security Measures

Schedule 3 - Sub-Processors

Schedule 4 - EU Model Contract Clauses

SCHEDULE 1

CATEGORIES OF DATA

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

1. Data Exporter:

The data exporter is the Customer and its end users.

2. Data Importer:

The data importer is ActiveNav, a provider of a software service.

3. Categories of Data:

The personal data transferred that is included in e-mail, documents, and other data in an electronic form in the context of the Online Services or Professional Services. ActiveNav acknowledges that, depending on Customer's use of the Online Service or Professional Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example username, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details).
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of Wi-Fi access points);
- Photos, video and audio;

- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);

- Device identification (for example IMEI-number, SIM card number, MAC address);

- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);

- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);

- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);

- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);

- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;

- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or

- Any other personal data identified in Article 4 of the GDPR.

4. Data Subjects:

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. ActiveNav acknowledges that, depending on Customer's use of the Online Service or Professional Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;

- Dependents of the above;

- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);

- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;

- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;

- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);

- Minors; or

- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

5. Processing Operations:

a. With respect to Customer's data, the parties acknowledge and agree that Customer is the 'data controller' (as defined in the Data Protection Legislation) and ActiveNav is a 'data processor' (as defined in the Data Protection Legislation). Customer will comply with its obligations as a data controller and ActiveNav will comply with its obligations as a data processor under the Agreement.

b. ActiveNav will only process Customer data in the performance of the Services in accordance with Customer's written instructions as documented in this DPA.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

ActiveNav must have in place security safeguards that are designed to conform to or exceed industry best practices regarding the protection of the confidentiality, integrity, and availability of customer data. These information security safeguards must be materially consistent with, or more stringent than, the safeguards described in this Schedule.

1. Web-Application Security Controls:

a. ActiveNav's Information Security Management System (ISMS) is structured around the ISO27001:2017 framework; designed to preserve the confidentiality, integrity, and availability of information. This is managed by an information security team, and is bolstered by data protection, privacy, and compliance programs which are overseen by our Chief Technology Officer (CTO).

b. Set out below are some of the controls and measures ActiveNav utilizes in the protection of information:

- Data is transferred over Transport Layer Security (TLS)
- Data is secured at rest using Advanced Encryption Standard (AES)
- Platform passwords are one-way hashed

2. Encryption:

a. ActiveNav stores customer data on ActiveNav-controlled IaaS and PaaS services, housed within the Microsoft Azure Commercial Cloud. The Azure cloud services are independently verified to standards including, but not limited to, ISO 27001, SOC 1, 2 & 3, FedRAMP, HIPAA, and PCI DSS. The Azure Commercial Cloud is composed of a globally distributed datacenter infrastructure, supporting thousands of online services and spanning more than 100 highly secure facilities worldwide, preserving data residency, and offering comprehensive compliance and resiliency for customers. ActiveNav encrypts customer data at rest using Azure Disk Encryption for Linux or Azure Transparent Data Encryption, which use FIPS 140-2 approved algorithms (AES-256), with encryption keys managed by the Azure Key Vault service.

b. ActiveNav utilizes HTTPS for securing data in transit and web server to web browser communications. When a user accesses the web interface via an internet browser, the HTTP session is redirected to HTTPS protocol using a Transport Layer Security (TLS 1.2) or higher connection.

c. ActiveNav's systems and networks are constantly monitored for security incidents, system health, network and traffic anomalies, and availability. ActiveNav performs periodic internal web application vulnerability assessments to ensure security controls are properly applied and operating effectively as designed. On at least an annual basis, ActiveNav performs external vulnerability assessments using third-party web applications. The scope of these external audits assesses compliance with the Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities. Vulnerability assessment results are incorporated into the ActiveNav Secure Software Development Lifecycle (SSDLC) to remediate vulnerabilities and internally tracked through resolution.

d. ActiveNav has an experienced security team with certifications that include (ISC)² Certified Cloud Security Professional Certified and other Microsoft Azure Professional Certifications.

SCHEDULE 3

SUB-PROCESSORS

ActiveNav's list of Sub-processors (to be updated from time to time in accordance with the terms in the DPA):

- Microsoft Corporation (third-party hosting provider)
- Salesforce.com (sales opportunity management)
- Microsoft Office 365 (email communications)
- Dropbox (document storage)
- HubSpot (product support and marketing automation)

SCHEDULE 4

MODEL CONTRACT CLAUSES

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For purposes of Article 26(2) of Directive 95/46/EC for the transfer of person data to processors established in third countries which do not ensure an adequate level of data protection.

Clause 1 – Definitions

For the purposes of the Clauses:

a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject', and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b. 'the data exporter' *means* the controller who transfers the personal data;

c. 'the data importer' *means* the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d. 'the sub-processor' *means* any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses, and the terms of the written subcontract;

e. 'the applicable data protection law' *means* the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f. 'technical and organizational security measures' *means* those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 – Details of the Transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in **Schedule 1** which forms an integral part of the Clauses.

Clause 3 – Third-Party Beneficiary Clause

a. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(a) and (b), Clause 7, Clause 8(b), and Clauses 9 to 12 as third-party beneficiary.

b. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

c. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

d. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 – Obligations of the Data Exporter

The data exporter agrees and warrants:

a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in **Schedule 2** to this contract;

d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e. that it will ensure compliance with the security measures;

f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(c) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h. to make available to the data subjects upon request a copy of the Clauses, with the exception of **Schedule 2**, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5 – Obligations of the Data Importer

The data importer agrees and warrants:

a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c. that it has implemented the technical and organizational security measures specified in **Schedule 2** before processing the personal data transferred;

d. that it will promptly notify the data exporter about:

   i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

   ii. any accidental or unauthorized access, and

   iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required

professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of **Schedule 2**, which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i. that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 – Liability

a. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

b. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

c. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

d. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs (a) and (b), arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 – Mediation and Jurisdiction

a. The data importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority, or

   ii. to refer the dispute to the courts in the Member State in which the data exporter is established.

b. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 – Cooperation with Supervisory Authorities

a. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

b. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

c. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph (b). In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 – Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 – Variation of the Contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required if they do not contradict the Clause.

Clause 11 – Sub-Processing

a. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

b. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph (a) of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

c. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph (a) shall be governed by the law of the Member State in which the data exporter is established.

d. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 – Obligation After Termination of Personal Data Processing Services

a. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

b. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph (a).