Gainsight Client Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of, and is subject to the Master Subscription and Services Agreement or other written or electronic agreement between Client and Gainsight, Inc. ("**Gainsight**") for the provision of Services to Client **("Agreement")** and applies where, and to the extent that, Gainsight processes Client Data (defined below) on behalf of Client when providing Services under the Agreement. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

By signing this DPA, Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where otherwise indicated, the term "**Client**" shall include the Client and its Controller Affiliates.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"CCPA" means the California Consumer Protection Act of 2018, upon the effective date thereof and as may be amended from time to time.

"**Client Data**" means any personal data that Gainsight processes on behalf of Client in the course of providing Services, and includes "personal information" as defined in the CCPA.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

"**Controller Affiliates**" means any of Client's Affiliate(s): (a) (i) that are subject to Data Protection Laws of the EEA, and (ii) permitted to use the Services pursuant to the Agreement between Client and Gainsight, but have not signed their own ordering document and are not a "Client" as defined under the Agreement, (b) if and to the extent Gainsight processes Client Data for which such Affiliate(s) qualify as the controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to a party and its processing of Personal Data under the Agreement, including, where applicable, GDPR (or in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data protection and privacy as a consequence of the United Kingdom leaving the European Union); in each case, as may be amended, superseded or replaced.

"**EEA**" means for the purposes of this DPA the European Economic Area, United Kingdom and Switzerland.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

"**Model Clauses**" means the Standard Contractual Clauses (Processors) (2010/87/EU): Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of

the Council (notified under document C(2010) 593), which do not ensure an adequate level of data protection.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification programs operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016, and by the Swiss Federal Council respectively (as may be amended, superseded or replaced).

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client Data.

"**Services**" means the generally available Gainsight product or service provided by Gainsight to Client pursuant to the Agreement.

"**Sub-processor**" means any Processor having access to Client Data and engaged by Gainsight to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Gainsight Affiliates but shall exclude any employee, consultant or contractor of Gainsight.

"**controller**", " **processor**", "**processing**" and "**personal data**" shall have the meanings given to them in the GDPR.

2. Roles and Scope of Processing

2.1 **Scope of this DPA.** This DPA applies where and only to the extent that Gainsight processes Client Data on behalf of Client in the course of providing Services to the Client pursuant to the Agreement.

2.2 **Role of the Parties**. As between Gainsight and Client, Client is either the data controller of Client Data, or if Client is acting on behalf of a third party data controller, then a data processor, and Gainsight shall process Client Data only as a data processor acting on behalf of Client and, with respect to the CCPA, as a "service provider" as defined therein. Gainsight will only process Client Data for the following purposes: (i) processing to perform any steps necessary for the performance of the Agreement; (ii) processing to provide the Services in accordance with the Agreement; (iii) processing initiated by end users in their use of Services; and (iv) processing to comply with other reasonable instructions provided by Client (e.g. via email or support tickets) that are consistent with the terms of this DPA (individually and collectively, the "**Purpose**") and only in accordance with Client's documented lawful instructions.

2.3 **Processing Instructions.** The parties agree that (i) the Agreement (including this DPA) sets out Client's complete and final instructions to Gainsight for the processing of Client Data; and (ii) processing outside the scope of these instructions (if any) will require prior written agreement between Client and Gainsight. Client shall ensure its instructions are lawful and that the processing of Client Data in accordance with such instructions will not violate applicable Data Protection Laws.

2.4 **Details of Data Processing**

(a) Subject matter: The subject matter of the data processing under this DPA is the Client Data.

(b) Duration: As between Gainsight and Client, the duration of the data processing under this DPA is the term of the Agreement.
(c) Purpose: Gainsight shall process Client Data only for the Purpose.
(d) Nature of the processing: Gainsight performs cloud hosting for its Customer Success management platform, with associated insight and analytics solutions, and such other services, as more particularly described in the Agreement.
(e) Categories of data subjects: prospects and customers (past, potential, present and future) of Client; employees or other contact persons (past, potential, present and future) of Client's prospects, customers, business partners and vendors; employees or other contact persons (past, potential, present and future) of Client (who are natural persons); Client's end-users (past, potential, present and future) authorized to use the Services.
(f) Types of Client Data: The types of Client Data are determined and controlled by Client in its sole discretion and may include personal contact data (name, title, address, phone number, email address) and other personal data subject to the conditions of the Agreement.

2.5 **Client Processing of Client Data.** Client agrees that it: (i) will comply with its obligations under Data Protection Laws in respect of its processing of Client Data; and (ii) has provided notice and obtained (or will obtain) all consents and rights necessary for Gainsight to process Client Data pursuant to the Agreement and this DPA.

3. Subprocessing

3.1 **Authorized Sub-processors.** Client agrees that in order to provide the Services, Gainsight may engage Sub-processors to process Client Data. Client specifically authorizes the engagement of those Sub-processors listed at https://www.gainsight.com/policy/sub-processors ("Sub-processor Site").

3.2 **Sub-processor Obligations.** Where Gainsight authorizes any Sub-processor as described in Section 3.1:

(a) Gainsight will restrict the Sub-processors access to Client Data only to what is necessary to assist Gainsight in providing or maintaining the Services and will prohibit the Sub-processor from accessing Client Data for any other purpose. Gainsight will enter into a written agreement with the Sub-processor imposing data protection obligations no less protective of Client Data as this DPA to the extent applicable to the nature of the services provided by such sub-processor. Gainsight will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Gainsight to breach any of its obligations under this DPA.

(b) Gainsight will provide ten (10) days' prior notice via the Sub-processor Site if it intends to make any changes to its Sub-processors. Client may object in writing within five (5) days to Gainsight's appointment of a new Sub-processor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties cannot agree a mutually acceptable resolution, Client shall as its sole and exclusive remedy have the right to terminate the Agreement. Any fees paid at the date of termination shall not be refunded.

4. Security Measures and Security Incident Response

4.1 **Security Measures.** Gainsight has implemented and will maintain appropriate technical and organizational security measures to protect Client Data from Security Incidents and to preserve

the security and confidentiality of the Client Data ("**Security Measures**"). The Security Measures applicable to the Services are set forth in **Annex A**, as updated or replaced from time to time in accordance with Section 4.2.

4.2 **Updates to Security Measures.** Client is responsible for reviewing the information made available by Gainsight relating to data security and making an independent determination as to whether the Services meet Client's requirements and legal obligations under Data Protection Laws. Client acknowledges that the Security Measures are subject to technical progress and development and that Gainsight may update the Security Measures from time to time.

4.3 **Personnel.** Gainsight restricts its personnel from processing Client Data without authorization by Gainsight as set forth in the Security Measures and shall ensure that any person who is authorized by Gainsight to process Client Data is under an appropriate obligation of confidentiality.

4.4 **Client Responsibilities.** Notwithstanding the above, Client agrees that except as provided by this DPA, Client is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Client Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Client Data uploaded to the Services.

4.5 **Security Incident Response.** Upon becoming aware of a Security Incident, Gainsight will notify Client without undue delay and, in any case, where feasible, within seventy-two (72) hours after becoming aware. Gainsight will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Client to fulfil its obligations as controller and will also take reasonable steps to contain, investigate, and mitigate any Security Incident.

5. Audits

5.1 **Audit reports**. Client acknowledges that Gainsight is regularly audited against SOC 2 Type II – standards by independent third-party auditors. Upon Client's written request, Gainsight will provide a summary copy of its then current SOC II Type 2 report ("**Report**") to Client, which Reports shall be subject to the confidentiality provisions of the Agreement. Gainsight shall also provide written responses (also on a confidential basis) to all reasonable requests for information made by Client relating to Gainsight's processing of Client Data, including responses to information and security audit questionnaires submitted to it by Client and that are necessary to confirm Gainsight's compliance with this DPA, provided that Client shall not exercise this right more than once per calendar year (except that this right may also be exercised in the event Client is expressly requested or required to provide this information to a data protection authority, or Gainsight has experienced a Security Incident, or other reasonably similar basis).

5.2 **Client Audits**. Client agrees to the provision of the Report and compliance with Section 5.1 above by Gainsight in fulfilment of any audit cooperation responsibilities that may apply to Gainsight under Data Protection Laws. Notwithstanding the foregoing, where required under any applicable Data Protection Laws or where a data protection authority requires under applicable Data Protection Law, Client may, on giving at least thirty (30 days) prior written notice, request that a third-party (at Client's expense) conduct an audit of Gainsight's facilities, equipment, documents and electronic data relating to the processing of Client Data under the Agreement to the extent necessary to inspect and/or audit Gainsight's compliance with this DPA, provided that: (i) Client shall not exercise this right more than once every calendar year;

(ii) such additional audit enquiries shall not unreasonably impact in an adverse manner Gainsight's regular operations and do not prove to be incompatible with applicable Data Protection Laws or with the instructions of the relevant data protection authority; and (iii) before the commencement of such additional audit, the parties shall mutually agree upon the scope, timing and duration of the audit. Without prejudice to the foregoing, Gainsight will provide all assistance reasonably requested by Client to accommodate Client's request.

6. International Transfers

6.1 **Location of Processing.** Gainsight may transfer (directly or via onward transfer) and process Client Data anywhere in the world where Gainsight or its Sub-processors maintain data processing operations, provided that Gainsight will at all times ensure that such transfers are done in compliance with the requirements of applicable Data Protection Laws and this Section 6.

6.2 **Data Transfers.** To the extent that Gainsight is a recipient of any Client Data under the Agreement that is protected by Data Protection Laws applicable to the EEA, and such Client Data is being transferred to a country that does not provide an adequate level of protection under applicable Data Protection Laws, the parties agree that Gainsight shall provide an adequate protection and/or appropriate safeguards for such Client Data by complying with the following transfer mechanisms:

(a) **Privacy Shield**. Gainsight has self-certified its compliance with Privacy Shield and accordingly Gainsight agrees to protect such Client Data in accordance with the requirements of the Privacy Shield Principles. If Gainsight is unable to comply with this requirement, Gainsight will inform Client.

(b) **Standard Contractual Clauses**. In the event the Privacy Shield does not apply to the transfer, is not accepted as a valid transfer mechanism under Data Protection Laws, is invalidated and/or Gainsight is no longer certified under Privacy Shield, Gainsight agrees to abide by and process the Client Data in compliance with the Model Clauses, which are incorporated by reference and form an integral part of this DPA. For the purposes of the Model Clauses, the parties agree that: (i) Gainsight is a "data importer" and Client is the "data exporter" (notwithstanding that the Client may be an entity located outside the EEA); (ii) Appendix 1 and 2 of the Model Clauses are replaced by Appendix 1 and 2 on Annex B of this DPA; and (iii) Appendix 3 on Annex B of this DPA shall form and be added as an Appendix 3 to the Model Clauses.

7. Return or Deletion of Data

7.1 Upon termination or expiration of the Agreement, Gainsight shall delete all Client Data in its possession or control. This requirement shall not apply to the extent Gainsight is required by applicable law to retain some or all of the Client Data, or to Client Data it has archived on back-up systems, which Client Data Gainsight shall securely isolate and protect from any further processing, except to the extent required by law.

8. Cooperation

8.1 To the extent that Client is unable to independently access the relevant Client Data within the Services, Gainsight shall, taking into account the nature of the processing, provide reasonable cooperation to assist Client in responding to any requests from individuals or applicable data

protection authorities relating to the processing of personal data under the Agreement. In the event that any such request is made to Gainsight directly, Gainsight shall not respond to such communication directly without Client's prior authorization, unless legally compelled to do so. If Gainsight is required to respond to such a request, Gainsight will promptly notify Client and provide it with a copy of the request unless legally prohibited from doing so.

8.2 If a law enforcement agency sends Gainsight a demand for Client Data (for example, through a subpoena or court order), Gainsight will attempt to redirect the law enforcement agency to request that Client Data directly from Client. As part of this effort, Gainsight may provide Client's basic contact information to the law enforcement agency. If compelled to disclose Client Data to a law enforcement agency, then Gainsight will give Client reasonable notice of the demand to allow Client to seek a protective order or other appropriate remedy unless Gainsight is legally prohibited from doing so.

8.3 To the extent Gainsight is required under Data Protection Laws applicable to the EEA, Gainsight will provide reasonably requested information regarding the Services to enable the Client to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

9. Controller Affiliates

9.1 **Contractual Relationship**. The parties acknowledge and agree that, by executing the DPA, Client enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between Gainsight and each such Controller Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10 below. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Client.

9.2 **Communication**. The Client entity that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Gainsight under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

9.3 **Rights of Controller Affiliates**. If a Controller Affiliate becomes a party to the DPA with Gainsight, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against Gainsight directly by itself, in which case the parties agree that: (i) solely the Client entity that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Client entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together.

10. Limitation of Liability

10.1 Any claim or remedies the Client or a Controller Affiliate may have against Gainsight and its respective employees, agents and Sub-processors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Client; (iii) under GDPR, including any claims relating to damages paid to a data subject; and (iv) breach of its obligations under the Privacy Shield and/or Model Clauses (as applicable), will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement.

10.2 For the avoidance of doubt, Gainsight and its Affiliates' total liability for all claims from the Client and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Client and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Client and/or to any Controller Affiliate that is a contractual party to any such DPA.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. General

11.1 No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

11.2 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.3 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

11.4 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

Annex A

Security Measures

Technical and organizational security measures to be implemented by Gainsight:

A. Annual Evidence of Compliance

1. ***Third Party Security Audit:*** Gainsight shall continue to be annually audited against the SOC 2 Type II standard, at Gainsight's expense. The audit shall be completed by an independent third-party. Upon Client's written request, Gainsight will provide a copy of the resulting annual audit report. Although that report provides an independently audited confirmation of Gainsight's security posture annually, the most common points of interest are further detailed below. Gainsight shall provide Client with this initial evidence of compliance within thirty (30) days of written request and annually upon written request.

2. ***Executive Summary of Web Application Penetration Test:*** Gainsight shall continue to annually engage an independent, third-party to perform a web application penetration test. Upon Client's written request, Gainsight shall provide the executive summary of the report to Client. Gainsight shall address all vulnerabilities in the findings of the report within a reasonable, risk-based timeframe. The third-party web application penetration test shall be done at least annually and vulnerabilities as defined by industry standards shall be remediated within a reasonable risk-based timeframe or identified as a residual risk where action(s) should be taken to remediate as soon as possible. Gainsight shall provide Client with this initial evidence of compliance within thirty (30) days of written request.

3. ***Security Awareness Training:*** Gainsight shall provide annual Security Awareness training to all personnel. Security Awareness training shall address security topics to educate users about the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms. Training materials should address industry standard topics which include, but are not limited to:

    - The importance of information security, the consequences of information security failures and how to report a security breach.
    - Physical controls such as visitor protocols, safeguarding portable devices and proper data destruction.
    - Logical controls related to strong password selection/best practices.
    - How to recognize social engineering attacks such as phishing.

4. ***Vulnerability Scan:*** Gainsight shall ensure that vulnerability scans are completed at minimum quarterly using an industry standard vulnerability scanning tool. All cloud hosted systems shall be scanned, where applicable and where approved by cloud service provider.

B. Security

1. Process-Level Requirements

a. Gainsight shall implement user termination controls that include access removal / disablement promptly upon termination of staff.

b. Documented change control process will be used to record and approve all major releases in Gainsight's environment.
c. Gainsight shall have and maintain a patch management process to implement patches in a reasonable, risk-based timeframe.

2. Network Requirements

a. Gainsight shall use firewall(s), Security Groups/VPCs, or similar technology to protect servers storing Client Data.
b. Gainsight shall ensure that vulnerability scans are completed at minimum quarterly using an industry standard vulnerability scanning tool. All cloud hosted systems shall be scanned, where applicable and where approved by the cloud service provider. Findings shall be addressed within a reasonable, risk-based timeframe.

3. Hosting Requirements

a. Where Gainsight handles Client Data, servers shall be protected from unauthorized access with appropriate physical security mechanisms including, but not limited to, badge access control, secure perimeter, and enforced user provisioning controls (i.e. appropriate authorization of new accounts, timely account terminations and frequent user account reviews). These physical security mechanisms are provided by data center partners such as, but not limited to, AWS, Salesforce and Google.
b. Cloud environment Data Segregation: Gainsight will virtually segregate all Client Data in accordance with its established procedures. The Client instance of Service may be on servers used by other non-Client instances.

4. Application-Level Requirements

a. Gainsight shall maintain documentation on overall application architecture, process flows, and security features for applications handling Client Data.
b. Gainsight shall employ secure programming techniques and protocols in the development of applications handling Client Data.
c. Gainsight shall employ industry standard scanning tools to identify application vulnerabilities prior to release.

5. Data-Level Requirements

a. Encryption and hashing protocols used for Client Data in transit and at rest shall support NIST approved encryption standards (e.g. SSH, TLS).
b. Gainsight shall ensure laptop disk encryption.
c. Gainsight shall ensure that access to information and application system functions is restricted to authorized personnel only.
d. Client Data stored on archive or backup systems shall be stored at the same level of security or better than the data stored on operating systems.

6. End User Computing Level Requirements

a. Gainsight shall employ an anti-virus solution with daily signature updates for end user computing devices which connect to the Client network or handle Client Data.
b. Gainsight will have a policy to prohibit the use of removable media for storing or carrying Client Data. Removable media include flash drives, CDs, and DVDs.

7. Compliance Requirements

a. Gainsight shall adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to building access control, employee security awareness education, etc.
b. Gainsight will, when and to the extent legally permissible, perform criminal background verification checks on all of its employees that provide services to Client prior to obtaining access to Client Data. Such background checks shall be carried out in accordance with relevant laws, regulations, and ethics.
c. Gainsight will maintain an Information Security Policy (ISP) that is reviewed and approved annually at the executive level.

8. Shared Responsibility: Gainsight's Services require a shared responsibility model. For example, Client must maintain controls over Client user accounts (such as disabling/removing access when a Client employee is terminated, establishing password requirements for Client users, etc.).

Annex B

Appendices to the Model Clauses

Appendix 1:

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter: The data exporter is the entity identified as the "Client" in the Data Processing Addendum in place between data exporter and data importer to which these Clauses are appended ("**DPA**") on page 1 of these Clauses and is a customer of the data importers Services (defined below). The data exporter and its affiliates shall be transferring personal data to the data importer in connection with the Services.
Data importer: The data importer is Gainsight, Inc. The data importer provides a platform hosted customer management success platform and associated customer insight and analytics solutions ("**Services**") which processes Client Data upon the instruction of the Client under the Agreement.
Description of Data Processing: Section 2.4 of the DPA (Details of Processing) sets forth a description of the categories of data subjects, categories of data, and processing operations. The personal data transferred concerns no special categories of data.

Appendix 2:

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5 (c) are set forth in Annex A of the DPA.

Appendix 3:

This Appendix forms part of the Clauses and must be completed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").
4. If after the Cure Period, the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Audits) of the DPA to which these Clauses are appended.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 3 (Subprocessing) of the DPA.