Addendum Addressing Article 28 GDPR (Processor Terms) and Incorporating Standard Contractual Clauses for Controller to Processor Transfers of Personal Data from the EEA to a Third Country

This Data Protection Addendum ("**Addendum**") forms part of the Subsentio-Client MSA ("**Principal Agreement**") between: (i) Subsentio, LLC **("Vendor")** acting on its own behalf and as agent for each Vendor Affiliate; and (ii) [Client Name] ("**Company**") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. **Definitions**

1.1 In this Addendum, the following terms shall have the meanings set out below:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.5 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 12 below;

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.12 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated in that Annex;

1.1.13 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.14 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation.

2. **Authority**

Vendor warrants and represents that it has duly and effectively authorized its Vendor Affiliates to Process Company Personal Data on behalf of one or more Company Group Members.

3. **Processing of Company Personal Data**

3.1 Vendor and each Vendor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2 not Process Company Personal Data other than pursuant to the Principal Agreement unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR. Company and Vendor may make reasonable amendments to Annex 1 from time to time as they reasonably consider necessary to meet those requirements.

4. **Vendor and Vendor Affiliate Personnel**

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. **Security**

5.1 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, Vendor and each Vendor Affiliate shall in relation to the Company 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.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Subprocessing**

6.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as of the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4. Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor.

6.2 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.2.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.2.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.2.3 Vendor and each Vendor Affiliate shall ensure that each Subprocessor Processes Company Personal Data as if it were party to this Addendum in place of Vendor.

7. **Data Subject Rights**

7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing the measures of this subsection, insofar as this is possible, for the fulfilment of the Company Group Members' obligations to respond to requests from Data Subjects.

7.2 Vendor shall:

7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law regarding Company Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate.

8. **Personal Data Breach**

8.1 Vendor shall notify Company without undue delay if Vendor or any Subprocessor becomes aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. **Data Protection Impact Assessment and Prior Consultation**

Vendor and each Vendor Affiliate shall provide each Company Group Member with Vendor's most current data protection impact assessment upon request by Company.

10. **Deletion or return of Company Personal Data**

10.1 Upon termination of the Principal Agreement, Vendor and each Vendor Affiliate shall promptly delete Company's Personal Data unless, by the termination date, Company requests the return of such Personal Data.

10.2 If Company requests the return of Company's Personal Data, Vendor and each Vendor Affiliate shall return the Personal Data in a secure manner.

10.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11. **Audit rights**

11.1 Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 In recognition of Vendor's security and privacy standards, audits and inspections under this subsection shall be conducted via information exchanges, as opposed to physical entry into any Vendor or Vendor Affiliate premises, and shall not include the audit or inspection of

proprietary information such as hardware, software, financial data, client names, or client subscriber information.

11.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under this section.

12. **Restricted Transfers**

12.1 Each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect when:

12.2.1 the data exporter becomes a party to them;

12.2.2 the data importer becomes a party to them; and

12.2.3 Company commences the relevant Restricted Transfer.

12.3 The purpose of this Section is to transfer Company Personal Data without breach of applicable Data Protection Law.

12.4 Company warrants and represents that it shall transfer Company Personal Data to Vendor or a Vendor Affiliate only in accordance with the Principal Agreement and only upon providing a written authorization for Vendor or a Vendor Affiliate to process the Company Personal Data.

13. **General Terms**

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate’s obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed

otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

13.4 Company and Vendor may from time to time amend this Addendum to modify the Standard Contractual Clauses as need to allow Restricted Transfers to be made (or continue to be made) without breach of Data Protection Law. If either Party requests a modification of this Addendum the other Party shall promptly co-operate to negotiate such modification in good faith.

13.5 Should any provision of this Addendum be invalid or unenforceable, the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

[Company]

Signature _____

Name _____

Title _____

Date Signed _____

[Vendor]

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Pursuant to GDPR Article 28(3), the following describes the Processing of Company Personal Data by Vendor and Vendor Affiliates.

I. DATA CLASSIFICATION

Subsentio organizes data into three categories:

(1) national security;
(2) personal/case sensitive; and
(3) and non-sensitive.

In the United States, national security data primarily includes court orders, national security letters, and related subscriber information and communications disclosed under the Foreign Intelligence Surveillance Act (FISA). In other countries, national security data includes the same type of information and communications disclosed under statutes that parallel FISA.

Subsentio's definition of personal/case sensitive data tracks the GDPR definition of "personal data." It is "data from which a living individual can be identified or identifiable (by anyone), whether directly or indirectly, by all means reasonably likely to be used." Personal data includes the names, addresses, online identifiers, credit card payment information and any other "subscriber information" belonging to communication service provider (CSP) subscribers. The definition also includes communications content, regardless of whether the content is transmitted in real time (e.g. a telephone call) or stored (e.g. email). Another form of personal data is communications transactional information, also known as metadata. The metadata of a communication (e.g. a call or broadband session) indicates the time and date of the communication, as well as the related duration. Finally, personal data includes a subscriber's wireless location, whether determined through cell site triangulation or GPS readings.

Personal data is case sensitive when gathered by an LEA pursuant to a criminal or national security investigation. Subsentio does not disclose case sensitive data to anyone other than the LEA authorized to receive the data.

Even when personal data is processed for a civil proceeding, and is therefore not case sensitive, it still deserves a high level of privacy protection. In fact, there is only one privacy-related difference between a civil proceeding and a criminal/national security proceeding. In the civil context we may notify subscribers named in the instruments of due process that they are subject to data requests so they may take legal actions to protect the privacy of their data. For example, a subscriber may choose to file a motion to quash before the presiding court. We provide these notices if requested by our CSP clients, who are the principals in our agent-principal relationships. In the criminal/national security context we lack the flexibility of providing subscriber notices because the related instruments of due process routinely contain "do not disclose" orders to prevent leaks of case sensitive information to the targeted suspects.

Non-sensitive data is any data that does not fall in the categories of national security or personal/case sensitive.

II. DATA PROCESSING IN THE LAWFUL INTERCEPT (LI) SERVICE

The following GDPR policies govern Subsentio's LI service on behalf of its CSP clients in support of law enforcement agency (LEA) investigations.

A. LI Order Validation

When a US-based LI order is served on a client, Subsentio's Law Enforcement Liaison Division (LELD) forwards a copy of the order via secure transmission to Legal, and Legal reviews it for validity. The client and its counsel may also conduct a validation review. If the US-based LI order is issued pursuant to a national security investigation, only LELD will perform the review because they have the required security clearances. However, the client may decide to designate its own cleared personnel for this purpose. In either case, the designated validation shall be done at all times according to the policies and procedures agreed to by Subsentio and the client.

In an emergency investigation in the US, where an LEA alerts Subsentio to a life-or-death situation (or other threat of bodily harm) and claims there is no time to obtain regular LI authority, Subsentio follows the emergency procedure permitted under the US Wiretap Act. We document the LEA representations regarding the exigent circumstances and activate the LI solution only temporarily. After 48 hours, unless the LEA replaces the emergency LI authority with regular authority, Subsentio terminates the LI. Subsentio likewise follows the emergency LI procedures of foreign jurisdictions.

The handling of national security LI orders follows the applicable nation's national security laws. For example, in US national security investigations, LELD (not Legal) performs the LI order validation. In foreign national security investigations, only the client or its counsel would perform the validation.

If the validation process reveals a defect in a US order, LELD communicates the determination to the case agent. Where there is a defect in a foreign order, the client or its counsel would inform the case agent. In any event, the order is not implemented until and unless the defect is cured.

At the end of the validation process the client authorizes Subsentio to implement the LI order by sending Subsentio a signed service provider authorization form.

B. LI Order Implementation

Assuming the LI order is valid, LELD staff records the LI order information and contacts the LEA to arrange a secure connection (or store-and-forward delivery method) between the CSP network and the LEA monitoring point for transmission of the intercepted data. If Subsentio receives the contact information of an LEA agent to establish the connectivity, Subsentio would use the contact information only for that purpose.

To implement a US LI order, LELD staff first records the profile facts of the case, including the authorizing court, the authorized LEA, the type of LI ordered, the subscriber's unique

identifier (e.g. telephone number, IP address, MAC address), and the date. The record is then securely stored.

Next, LELD staff activates the CSP's LI solution in accordance with the LI order. Certain LI solutions involve technology that requires the technical expertise of the LAES Engineering staff. In those situations, the LAES Engineering staff will activate the solution to intercept the target or targets named in the order. On the LI expiration date, the LI solution is automatically deactivated pursuant to a setting programmed at the time of activation. The LI would continue for a longer period only if the CSP is served with a valid renewal order prior to the expiration date. LELD staff inserts the deactivation date in its record of the case and advises both the LEA and CSP of the deactivation time and date. LELD then files the record in secure storage.

In foreign jurisdictions that prohibit the transfer of personal information beyond their borders, Subsentio retains citizens of the host country to perform the LI work in-country. In foreign countries that lack such "data localization" laws, Subsentio protects the privacy of cross-border data transfers by entering into "standard contractual clauses," also known as "model clauses," with its international clients. The only item of personal information to be transferred under the model clauses is the suspect's unique identifier.

Certain LI implementations may span two or more jurisdictions. For example, in a cloud-based LI solution, the targeted data is intercepted at a data center instead of a switching office or session border controller. The data is then mediated and forwarded to the LEA monitoring point. In this scenario the suspect, the data center, and the LEA may be located in different countries. This is known as a "cross-border" intercept. The international community has not harmonized its LI jurisdictional laws to accommodate cross-border intercepts. As a result, a cross-border intercept may pose a conflict between the surveillance law of one country and the privacy law of another. Subsentio's policy is to minimize these conflicts as much as possible through coordination with the affected governmental authorities.

The communications Subsentio intercepts and delivers in the course of an LI are those processed by the CSP client network. Subsentio does not modify the data; it only formats the data to prepare it for delivery to the LEA. Most often, the formatting is performed in accordance with LEA/industry-recognized LI technical standards. Subsentio does not store LI data. In some LI solutions, data packets are buffered (temporarily held in a reserve area of memory) to ensure the accuracy of the delivery.

Subsentio observes the following LI security standards:

1. Subsentio's LI servers contain an OS-based firewall that restricts incoming traffic based on source IP addresses.
2. Only two ethernet communications ports are available on our LI servers and both involve a secure encapsulation and authentication process, port 22 (SSH) and 443 (HTTPS). Access to port 22 requires a Subsentio generated SSH RSA key with a passphrase. Access to port 443 requires Subsentio-issued public and private X.509 certificates.
3. Remote access requires a user ID with a strong/complex password management.
4. Provisioned targeting data on the servers is encrypted using a file-based AES-256 encryption.

5. LI servers and solution elements are actively monitored by our centralized web based network management system. The monitoring includes availability and performance checks and support alerts and notifications.
6. LI servers comply with our manufacture's application and OS recommended backup strategy.

IMPORTANT NOTE: Not all the above security hardening controls and measures apply to all Subsentio LI solutions. In most cases, only a subset of these elements would be applicable to Subsentio's overall LI product line.

III. DATA PROCESSING IN THE DATA RETENTION (DR) SERVICE

The following GDPR policies govern Subsentio's data retention service on behalf of its CSP clients in support of LEA investigations and civil proceedings.

In some jurisdictions (e.g. many European Union member states) the data retention statute mandates both data storage and data retrieval. In others (e.g. the U.S.) the law requires only data retrieval. Subsentio upholds the same privacy standards for both types of regulation.

Subsentio helps CSPs comply with their obligations to disclose stored (or "historic") communications records to LEAs and requesting civil parties upon valid request. Such records are collectively known as communications data records, or "CDRs".

A. DR Order Validation

When a US-based DR order is served on a client, the order is validated by a specially-trained employee (an Analyst). DR orders in national security investigations are also reviewed by the Analysts. For foreign-based DR orders in criminal and national security proceedings, the validation is performed by the client or its counsel.

In an emergency investigation in the US, if an LEA alerts Subsentio to a life-or-death situation (or other threat of bodily harm) and declares an emergency where there is no time to obtain regular DR authority, Subsentio would follow the emergency procedure permitted under the Electronic Communications Privacy Act. We would document the LEA representations regarding the exigent circumstances in the Subsentio platform known as the Legal Demand Tracker™ and then disclose the targeted records. Subsentio will likewise follow the emergency DR procedures of foreign jurisdictions.

If the validation reveals a defect in the DR order, the Analyst describes the defect to the case agent/LEA. Where there is a defect in a foreign order, the client or its counsel would inform the case agent/LEA. In any event, the order is not implemented until and unless the defect is cured.

B. DR Order Implementation

If the DR order is valid, the Analyst remotely and securely accesses the client's customer data repository, retrieves an automated report on the targeted CDRs, redacts from the report any CDRs not described in the order, attaches a certificate to the report to authenticate the data retrieval, transmits the combined package to the requesting party, and makes a record of the

transaction in Subsentio's secure Legal Demand Tracker™ (LDT) platform. Some clients prefer to accomplish the data retrieval step through a manual process. In that scenario, a designated point of contact at the client site retrieves the records and sends them to the Analyst for further processing.

Some countries prohibit CSPs from transferring CDRs outside their jurisdictions. For clients that are subject to such data localization laws, Subsentio and the client ensure that the CDRs remain in the jurisdiction. In these nations, Subsentio hires citizens of the foreign jurisdiction to perform the above DR processing tasks in-country.

Nations that impose data retention mandates regulate the types of CDRs that must be retained, as well as the timeframe of the retention. A commonly prescribed retention period is two years. Subsentio complies with these mandates. In the absence of a data retention mandate Subsentio stores the data for the period designated by the client. Subsentio recommends a period of two years. When the storage period expires, Subsentio securely destroys the data or returns it to the client.

In the unlikely event of a data breach Subsentio would alert the client based on pre-defined data breach notification requirements about the circumstances of the breach. The client would then activate its data breach notification procedure to alert the affected subscribers and interested government agencies.

In civil cases, when instructed by the client, Subsentio notifies the subscriber targeted by the DR request so the individual has an opportunity to oppose the disclosure. The person may file a motion to minimize or quash the due process. In gray-area cases, where it is unclear whether Subsentio should proceed with the disclosure, the analyst sends the targeted CDRs to the designated court representative under seal instead of the requesting party.

CDRs are retrieved from the client as is and assembled for disclosure without alteration, except for redactions needed to limit the scope of data disclosed to the scope of data described in the order.

Subsentio's LDT solution for DR incorporates the following security hardening controls and measures:

1. Analyst and support access: requires a Subsentio-owned X.509 SSL certificate, if cloud-based storage, Amazon Web Services (AWS) security group inbound controls based on source IP address and port, and user ID with strong/complex password management.
2. Data at rest: AES-256 volume encryption and automatic volume AES-265 encryption during data snapshot and SQL backup to long-term storage.
3. Alerts and notifications: on synchronization, snapshot, and SQL backup on successfully and failed events.
4. AWS monitoring and notifications on EC2 CPU utilization, status checks, and state changes.

Just as an LI order may trigger a cross-border intercept, a DR order may involve the cross-border disclosure of CDRs. The international community has not harmonized its DR jurisdictional laws to accommodate such cross-border requests. As a result, a cross-border request may pose a conflict between the surveillance law of one country and the privacy law of another.

Subsentio's policy is to minimize these conflicts as much as possible through coordination with the affected governmental authorities.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

Company and Vendor have agreed to the following Contractual Clauses (the Clauses) with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer (the Services) will involve the transfer of personal data to data importer. Data importer is located in the United States, which has not adopted the GDPR standards of adequate data protection. To ensure compliance with the GDPR, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

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 the General Data Protection Regulation (the GDPR).

(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 the data exporter's behalf after the transfer in accordance with the instructions and terms of these Clauses.

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 its 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 organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. Subject to the applicable requirements of due process in criminal investigations, national security investigations, and civil litigation, 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(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. Subject to the applicable requirements of due process in criminal investigations, national security investigations, and civil litigation, the data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), 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.

3. Subject to the applicable requirements of due process in criminal investigations, national security investigations, and civil litigation, the data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), 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 subprocessor shall be limited to its own processing operations under the Clauses.

4. Subject to the applicable requirements of due process in criminal investigations, national security investigations, and civil litigation, 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 organisational security measures specified in Appendix 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, unauthorised 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 the GDPR.

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) 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 Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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 organisational security measures specified in Appendix 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 unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. 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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. 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 subprocessor 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.

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. 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

1. 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.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. 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 as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. 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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 1 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing 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 the termination of personal data processing services

1. 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.

2. The data importer and the subprocessor 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 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Data subjects

The personal data transferred concern the following categories of data subjects:
Suspects in criminal investigations, suspects in national security investigations, and parties in civil court proceedings.

Categories of data

The personal data transferred concern the following categories of data:

The data importer organizes data into three categories: (1) national security; (2) personal/case sensitive; and (3) and non-sensitive. Within data categories one and two, the data exporter will, as needed to comply with applicable due process demands, transfer to the data importer an item of personal data, namely the suspect's unique identifier (e.g. telephone number, IP address, MAC address).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:
N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities:
The data importer shall use the above-described unique identifier to provision lawful surveillance on the data exporter's behalf. For a detailed description of the provisioning process, see Annex 1 of the Addendum to which this appendix is attached.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data importer will implement the technical and organizational security measures described at Annex 1 of the Addendum to which this appendix is attached.