Data Processing Addendum – AppColl, Inc.

This Data Processing Addendum (**"Addendum"**) forms part of the AppColl Service Agreement in regards to the Protection of Users Personal Data between AppColl, Inc. **("Vendor")** acting on its own behalf and as agent for each Vendor Affiliate, and you (**"Company"**) acting on your 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 Service Agreement. Except as modified below, the terms of the Service 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 Service Agreement. Except where the context requires otherwise, references in this Addendum to the Service Agreement are to the Service 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 and cognate terms shall be construed accordingly:

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 Service Agreement;

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

1.1.6.   **"Data Protection Laws"** means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

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 6.4.3 or 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 Service Agreement;

1.1.12.   "**Standard Contractual Clauses**" means the (Standard Contractual Clauses (processors)) (established by Commission Decision February, 5 2010) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. They include Appendices 1 and 2 attached to this DPA.

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 Service 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, and cognate terms shall be construed accordingly.

2.   Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

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 on the relevant Company Group Member's documented instructions 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 Service 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.   Appendix 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 (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Appendix 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Appendix 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

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 Service 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 Service Agreement.

6.2.   Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at 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.

6.3.   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. If, within 30 days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

6.3.1.   Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and

6.3.2.   where such a change cannot be made within 30 days from Vendor's receipt of Company's notice, notwithstanding anything in the Service Agreement, Company may by written notice to Vendor with immediate effect terminate the Service Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.

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

6.4.1.   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 Service Agreement;

6.4.2.   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;

6.4.3.   if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement 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, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.4.4.　provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5.　Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, 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 appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

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 in respect of 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 or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8.　**Personal Data Breach**

8.1.　Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming 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. Such notification shall as a minimum:

8.1.1.　describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.1.2.　communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3.　describe the likely consequences of the Personal Data Breach; and

8.1.4.　describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2.　Vendor shall cooperate 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 reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

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

10.1. Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within 60 days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

10.2. Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within 30 days of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within 60 days of the Cessation Date.

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.

10.4. Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within 65 days of the Cessation Date.

11. **Audit rights**

11.1. Subject to sections 11.2 to 11.4, 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 or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2. Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Service Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

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 section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its

personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1.   to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2.   outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

11.3.3.   for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

11.3.3.1.   Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or

11.3.3.2.   A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.

12.   Restricted Transfers

12.1.   Subject to section 12.3, 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 under section 12.1 on the later of:

12.2.1.   the data exporter becoming a party to them;

12.2.2.   the data importer becoming a party to them; and

12.2.3.   commencement of the relevant Restricted Transfer.

12.3.   Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

13.   General Terms

Governing law and jurisdiction

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 Service 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 Service Agreement.

Order of precedence

13.2. Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Service 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 Service 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 Service 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.

Changes in Data Protection Laws, etc.

13.4. Company may:

13.4.1. by at least 30 calendar days' written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2. propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5. If Company gives notice under section 13.4.1:

13.5.1. Vendor and each Vendor Affiliate shall promptly cooperate (and ensure that any affected Subprocessors promptly cooperate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and

13.5.2. Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6. If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7. Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8. Should any provision of this Addendum be invalid or unenforceable, then 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.

Applicability

13.9. Applicability of DPA. This DPA will apply only to the extent that Vendor processes Personal Data originating from the EEA on behalf of a Company or Company Affiliate located in the EEA.

APPENDIX 1 TO THE ADDENDUM & STANDARD CONTRACTUAL CLAUSES

DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Data subjects

The personal data transferred concern the following categories of data subjects:

- Licensed users of Vendor's service(s) (Users),
- Contact information of external subjects as provided by Users (Contacts)

Categories of data

The personal data collected by Vendor concern the following categories of data:

Field Name	Field Name	Field Name
Name	ResidenceCountry	NoOverdueReminders
Prefix	Citizenship	UsedBy
First	Fax	Organization
Middle	Phone	ReportsInto
Last	Mobile	GetsInventionAwards
Suffix	Email	Tags
Nickname	Skype	Keywords
ForeignNickname	URL	Technologies
Role	TaxID	AssociatedWith
HourlyRate	SmallEntity	CompetesWith
Client	USMilitaryService	PrivateNotes
Company	USPTORegNum	Aliases
ShortName	USPTOCustNum	Flag
Title	USPTODepAcc	RestrictedAccess
Street	Notes	Status
Street2	Modified	LastFirstMiddle
City	WireInstructions	LEDESTimekeeperCode
State	SpecialNotes	
PostalCode	Initials	
Country	StateOfIncorporation	
ResidenceCity	DisableReminders	
ResidenceState		

Vendor does not intentionally collect or process any special categories of data in the provision of its Services.

Vendor uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Service Agreement). These Sub-processors set out below provide cloud hosting and storage services; recurring billing services; assist in providing customer support; as well as incident tracking, and response services.

Entity Name	Corporate Location	Data Processed
Amazon	Washington, USA	All Customer Data collected as part of Vendor services (Users and Contacts)
SendinBlue	Paris, FRANCE	Email address, Name, Customer company name of Users (mailing list for announcements). Contacts are not exported.

Salesforce	Colorado, USA	Any data provided by User for Vendor to provide support services (customer support)
PayPal	California, USA	Name, Email address of Customer responsible for recurring billing of Vendor services (for those Customers that utilize the service)
PagerDuty	California, USA	Aggregated incident tracking and notification
Microsoft	Washington, USA	Any data provided by User to provide support and/or account services (emails)
Atlassian	California, USA	Any data provided by User for Vendor to improve services (bug tracking)
RingCentral	California, USA	Phone number, Caller ID; Any data provided by User for Vendor to provide support services (customer support)
Google Analytics	California, USA	Anonymized site usage data for internal marketing purposes

The nature and purpose of processing
The personal data transferred will be subject to the following basic processing activities (please specify):
- **Storage, backup, processing per Service Agreement.**

The subject matter and duration of the Processing of Company Personal Data
The subject matter and duration of the Processing of the Company Personal Data are set out in the Service Agreement and this Addendum.

The obligations and rights of Company and Company Affiliates
The obligations and rights of Company and Company Affiliates are set out in the Service Agreement and this Addendum.

APPENDIX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

This Appendix forms part of the Clauses and must be completed and signed 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):

1. TECHNICAL AND ORGANIZATIONAL MEASURES
The following sections define the Vendor's current security measures. Vendor may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

- Physical Access Control

  - Vendor's systems are physically secured; more information can be found here: https://aws.amazon.com/compliance/soc-faqs/ and https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/

- System Access Control

  - All Vendor systems require appropriate access authentication and authorization. Vendor utilizes multiple security products to prevent unauthorized access. Vendor performs 3rd party security audits no less than twice annually.

- Data Access Control

  - Vendor support personnel access personal information only as part of providing customer support related to specific user requests. Access to Company's data is logged.

- Data Transmission Control

  - Data is transmitted over secure protocols (such as TLS). Files are encrypted in transit and at rest. Customer database backups are encrypted in transit and at rest.

- Data Input Control

  - Users have control over their own data. Users have abilities to delete, modify, and download data. Audit logs are available for inspection.

- Job Control

  - Vendor may transmit, analyze, or process personal data to provide services per Service Agreement. Vendor may transmit, analyze, or otherwise process anonymized and/or aggregated Company data in order to improve services.

- Availability Control

  - Vendor maintains redundant systems to provide backup services.

- Data Separation Control

- Vendor may, in order to provide or improve services, analyze data across multiple customers. Data is either anonymized, aggregated, or otherwise de-identified.

- Data Integrity Control

  - Vendor transmits data within Vendor systems using secure protocols (i.e. TLS); transmitted data is encrypted at rest; Transmission activities are logged. Export activities utilize secure protocols (i.e. TLS).