**EXHIBIT [X]**

**DATA PROTECTION ADDENDUM**

This Data Protection Addendum, (“**DPA**”) made between AlertEnterprise, Inc. (“**ALERT**”) and [CUSTOMER] (**“Customer”**) (together, the “**Parties**”), forms part of the Software as a Service and Managed Services Agreement between ALERT and Customer (“**Agreement**”) and reflects the Parties’ agreement regarding the Processing of Customer Personal Data.

# Definitions

## The terms “**Controller,**” “**Data Subject,**” “**Personal Data,**” “**Personal Data Breach,**” “**Processing,**” “**Processor,**” “**Special Categories of Personal Data,**” “**Supervisory Authority,**” and analogous terms shall have the same meaning as in Data Protection Law (or where not defined in applicable Data Protection Law, shall have the meaning as in the GDPR).

## In this DPA, capitalized terms that are not defined herein shall have the meanings set out in the Agreement. The following terms shall have the meanings set out below (and cognate terms shall be construed accordingly):

### “**Customer Personal Data**” means any Personal Data that is Processed by ALERT on behalf of Customer pursuant to, or in connection with, the Agreement and this DPA; as between the Parties, all Customer Personal Data shall be, and shall remain the property of, Customer;

### “**Affiliate**”means an entity that owns or controls, is owned or controlled by, or is or under common control or ownership of Customer or ALERT, 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;

### **“Agreement”** has the meaning set out in the Preamble;

### **“CCPA”** means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020;

### “**Data Protection Law**” means all national, federal, state, provincial, or local privacy, cybersecurity, and data protection laws, together with any implementing or supplemental rules and regulations, applicable to the processing of Personal Data under this DPA, as amended or replaced from time to time;

### **“GDPR**” means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and associated national legislation;

### “**Member State**” means a member state of the European Economic Area (“**EEA**”);

### “**Restricted Transfer**”means a transfer or an onward transfer of Customer Personal Data where such transfer would be prohibited by Data Protection Law in the absence of an adequacy decision, a permitted derogation, or protection for the transferred Customer Personal Data provided by binding corporate rules, SCCs, or other mechanism specified under applicable Data Protection Law;

### “**SCCs**” means, as applicable to the relevant data transfer: (i) Module 2 of the standard contractual clauses set out in the [Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Counci](https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=uriserv:OJ.L_.2021.199.01.0031.01.ENG&toc=OJ:L:2021:199:TOC)l (“**Module 2 SCC**”), (ii) the UK IDTA, or (iii) such other terms intended to provide adequate protection to transferred personal data pursuant to Data Protection Law; in each case, as amended or replaced from time to time under the relevant Data Protection Law;

### **“Security Incident”** means (i) any Personal Data Breach affecting Customer Personal Data, or (ii) any other event resulting in the unauthorized or unlawful access to, use, disclosure, loss, alteration or destruction of Customer Personal Data;

### **“Services”** means the services provided by ALERT pursuant to, or in furtherance of, the Agreement;

### “**Subprocessor**” means any Processor (including any third party and any ALERT Affiliate, but excluding an employee of ALERT or an employee of any of its sub-contractors) appointed by, or on behalf of, the ALERT to Process Customer Personal Data;

### **“Third Country”** means: (i) with respect to GDPR, a country other than the Member States; (ii) with respect to the UK Data Protection Law, any country outside of the UK; and (iii) with respect to any other country, as provided in relevant Data Protection Law;

### “**UK Data Protection Law**” means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (“**UK GDPR**”), together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), and other Data Protection Laws in force from time to time in the United Kingdom; and

### "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

# Processing Obligations

## Customer is a Controller and ALERT is a Processor with respect to all Customer Personal Data. Where applicable Data Protection Law uses terms other than Controller and Processor, the appropriate terms shall be understood to apply as the context requires.

## Details of the Processing are set out in **Annex 1** to this DPA.

## Customer instructs ALERT (and authorizes ALERT to instruct each Subprocessor) to Process Customer Personal Data, including to transfer Customer Personal Data to a Third Country, subject always to ALERT complying with the terms of this DPA, as reasonably necessary to provide the Services.

## ALERT shall at all times comply with applicable obligations under Data Protection Law, and shall:

### process Customer Personal Data only as permitted by applicable Data Protection Law and for the specific purposes of the Processing as set out in **Annex 1** or as otherwise instructed by Customer, unless Processing is required by Data Protection Law to which the ALERT is subject, in which case ALERT shall inform Customer of that legal requirement before such Processing, unless that law prohibits such information on important grounds of public interest;

### promptly revert to Customer to seek clarification if the instructions issued by Customer are unclear, and inform Customer if, in ALERT’s opinion, such instructions infringe Data Protection Law;

### grant access to Customer Personal Data only to the extent necessary for performing the Services, and ensure that all persons authorized to process Customer Personal Data are appropriately trained, and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

### implement the technical and organizational measures specified in **Annex 2** to ensure the security of Customer Personal Data, taking due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for Data Subjects; and, further, if, at any time, an authority mandates specific additional measures, the Parties shall work together in good faith to implement such measures;

### where ALERT is obligated by Data Protection Law to maintain a record of Processing activities,ALERT shall maintain a record of its Processing activities conducted for and on behalf of Customer in accordance with Data Protection Law.

## **CCPA Terms.**

## To the extent that ALERT Processes any Customer Personal Data subject to the CCPA, ALERT agrees to the following:

### All Customer Personal Data disclosed by Customer to ALERT, or that ALERT receives or processes on Customer’s behalf, is disclosed or received only for limited and specified purposes, including for one or more business or commercial purposes as those terms are defined under the CCPA.

### ALERT shall not sell, share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Customer Personal Data received from, or on behalf of, Customer to any third party for monetary or other valuable consideration.

### ALERT shall not retain, use, or disclose Customer Personal Data received from, or on behalf of, Customer: (i) for any purposes (including, but not limited to, any commercial purpose) other than a business purposes specified in the Agreement, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and ALERT.

### ALERT may combine Personal Data that it receives from, or on behalf of, Customer with Personal Data that ALERT receives from, or on behalf of, another person, or collects from its own interaction with an individual, unless the combining of that personal information (i) would not be consistent with an individual's expectations, or (ii) is prohibited by regulations issued by the California Privacy Protection Agency. For purposes of this DPA, "combine" means to aggregate personal information about an individual into a single profile.

### If Customer provides ALERT with deidentified Personal Data, or if ALERT deidentifies Personal Data previously provided by Customer, ALERT agrees to take reasonable measures to ensure that the deidentified Personal Data cannot be associated with a consumer or household, and not attempt to reidentify the personal information.

### If ALERT determines it can no longer meet its obligations under the CCPA, it shall promptly notify Customer of this fact.

### ALERT certifies it understands the obligations and restrictions above and will comply with them.

# Subprocessing

## Customer hereby grants ALERT general written authorization to retain Subprocessors as needed to perform the Services. ALERT will provide 30 days’ notice to Customer prior to engaging a new Subprocessor. Should Customer reasonably object to the addition of a Subprocessor by ALERT within the 30-day window, the parties shall negotiate in good faith to find a suitable alternative Subprocessor. If no agreement is reached between the parties, Customer shall have the right to terminate the Agreement as it relates to the use of the objected-to Subprocessor by ALERT. ALERT’s current list of Subprocessors engaged in Processing of Personal Data on behalf of ALERT (Subprocessor List) can be found in **Annex 3**. Customer hereby consents to the Subprocessors listed in **Annex 3** hereto, subject to the conditions set out in Section 4.2.

## With respect to each Subprocessor, ALERT shall:

### include terms in the contract between ALERT and each Subprocessor that provides for, in substance, the same data protection obligations as those binding on ALERT under this DPA;

### remain fully liable to Customer for any act or omission of its Subprocessor;

### upon Customer request, provide Customer with a summary of the Processing to be undertaken by each Subprocessor;

### upon Customer’s request, provide a copy of its Subprocessor agreement(s), and any subsequent amendments (provided, ALERT may redact the text of the agreement to the extent necessary to protect trade secrets or other confidential information, including personal data);

## Where ALERT engages an ALERT Affiliate as a Subprocessor, such ALERT Affiliate may engage further Subprocessors subject to all the above terms and conditions.

# Security Incident

## ALERT shall notify Customer without undue delay, but after a reasonable period to allow ALERT to investigate and, if necessary, involve law enforcement, upon ALERT becoming aware of an actual Security Incident. ALERT shall provide Customer with sufficient information to allow Customer to meet its obligations to assess and report a Security Incident under applicable Data Protection Law, which may be provided in stages as it becomes available to ALERT, and shall include the following: (a) a description of the nature of the Security Incident, including details of any Subprocessors involved, the categories and numbers of Data Subjects concerned, and the categories of Customer Personal Data concerned; (b) the name and contact details of ALERT’s relevant contact from whom more information may be obtained; (c) the likely consequences of the Security Incident; and (d) the measures taken or proposed to be taken to address the Security Incident.

## ALERT shall co-operate with Customer and take such commercially reasonable steps to assist in the investigation, containment, and remediation of a Security Incident.

## In the event of a Security Incident, ALERT shall not inform any regulator without first obtaining Customer’s prior consent, unless required by a law to which ALERT is subject, in which case ALERT shall, to the extent permitted by such law (i) not refer to, or mention, Customer in any such information, and (ii) inform Customer of that legal requirement. For avoidance of doubt, Customer, as the Controller, retains the right and obligation to determine, in its sole discretion, whether notification of a Security Incident involving Customer Personal Data to Supervisory Authorities, individuals, or other persons is required.

# Assistance to Customer – Regulator Requests and Data Subject Rights

## Taking into account the nature of the Processing and the information available to ALERT, ALERT shall promptly notify Customer if it receives any complaint, communication, subpoena, warrant, court order, audit notice, or other request (“request”) from a Supervisory Authority, law enforcement, court, or tribunal in respect of Customer Personal Data. ALERT shall not respond to the request itself, unless authorized to do so by Customer after Customer has had a reasonable opportunity to evaluate the merits of the request. ALERT shall cooperate with and assist Customer (i) in relation to any communication from a Regulator, public authority, law enforcement, representative labor body, or a Supervisory Authority, and (ii) in ensuring compliance with GDPR Articles 32-36 or equivalent obligations under applicable Data Protection Law. Where such assistance is unduly burdensome, ALERT retains the right to charge Customer a reasonable administrative hourly fee to provide such assistance.

## ALERT will, in a manner consistent with the nature and functionality of the services provided in the Agreement and ALERT’s role as a Processor, provide mechanisms or reasonable support to Customer to enable Customer to respond to Data Subject requests to exercise their rights under applicable Data Protection Laws (“Data Subject Requests”). If ALERT receives a Data Subject Request or other complaint directly from a Data Subject regarding the Processing of Customer Personal Data, ALERT will promptly forward such request or complaint to Customer and not respond to the request itself, unless authorized to do so by Customer or required by applicable Data Protection Laws.

# Deletion or Return of Customer Personal Data

## Subject to Section 7.2, and as required under applicable Data Protection Law, upon Customer’s request ALERT shall promptly: (a) return a copy of all Customer Personal Data to Customer by secure file transfer; and (b) delete all Customer Personal Data, other than Customer Personal Data stored in backup locations, which shall be deleted pursuant to ALERT’s backup and retention schedules.

## ALERT may retain Customer Personal Data to the extent and for such period as required by Data Protection Law, provided that ALERT shall ensure the confidentiality of all such Customer Personal Data and ensure that such Customer Personal Data is only Processed for the purpose(s) specified in such law.

## Notwithstanding anything in this DPA or the Agreement to the contrary, until Customer Personal Data is Deleted or returned, ALERT and each ALERT Affiliate shall continue to ensure compliance with this DPA.

# Audit Rights

## Customer acknowledges that ALERT shall be regularly audited against industry security standards by independent third-party auditors. Upon request, ALERT shall supply Customer a summary of its most recent audit report(s), which reports shall be subject to the confidentiality provisions contained in the Agreement. Pursuant to applicable Data Protection Law, Customer, or its independent third-party auditor, may remotely audit ALERT’s security practices only if:

## ALERT has failed to use commercially reasonable efforts to provide evidence of its compliance with its obligations under this DPA or applicable Data Protection Law by providing summaries or copies of its independent audit reports,;

## A Personal Data Breach involving the Customer has occurred;

## An audit is formally requested by a supervisory authority or regulator; or

## Applicable Data Protection Law confers on Customer such a right, provided that Customer shall not conduct such an audit more than once in any 12-month period, unless applicable Data Protection Law requires otherwise.

## The rights set out in clause 8.1 will be exercised in accordance with the following principles:

### any audit will be exercised taking a risk-based approach, considering the context and the nature of the Services, and adhering to relevant, commonly accepted audit standards;

### if Customer or a Regulator appoints a third-party to exercise its audit rights, Customer or the Regulator will use reasonable efforts to verify that the third-party auditor’s personnel have acquired the right skills and knowledge to perform effective and relevant audits and assessments of the Services;

### Customer acknowledges that all of ALERT’ information technology infrastructure is cloud-based (hosted by ALERT’ Subprocessors), and staff work remotely. Therefore, Adhoc on-site audits are not possible. An on-site audit of ALERT’ datacenters may be requested by Customer by providing advance written notice in the event: (i) ALERT cannot provide sufficent evidence of its compliance with this DPA (as described above), and (ii) Customer can demonstrate. and ALERT agrees, that additional information required to demonstrate compliance with this DPA may be obtained through a datacenter visit. Customer will provide reasonable advance notice (in light of the nature and scope of the requested audit), unless prior reasonable notice is not possible due to an emergency or crisis situation;

### audits will be restricted to ALERT’s normal business hours, and will not reasonably interfere with ALERT’s business operations; and

### if the exercise of any audit right could, in ALERT’s reasonable opinion, create a risk for another ALERT customer’s environment, Customer and ALERT (or the Regulator, as applicable) may agree on an alternative way to address the request to provide a similar level of assurance.

## If an audit under this Section 8 results in a determination that ALERT has not established reasonable and adequate security controls for compliance with ALERT’s obligations under this DPA, such a finding shall not constitute a breach of the DPA or the Agreement provided ALERT remedies the deficiency within 30 business days.

# Restricted Transfers

## Customer (as “data exporter”) and ALERT (as “data importer”), with effect from the commencement of the relevant transfer, hereby enter into: (i) the Module 2 SCC, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to GDPR (subject to Section 9.2); and (ii) the UK IDTA, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to UK Data Protection Law (subject to Section 9.3). Further, until such time as the relevant jurisdiction(s) issue their own standard contractual clauses, the Module 2 SCCs shall apply in respect of any Restricted Transfer subject to any other Data Protection Law that regulates cross-border transfers of Personal Data.

## The parties agree that with respect to the Module 2 SCC:

### *Clause 7 – Docking clause* shall not apply;

### In *Clause 9 – Use of subprocessors*, Option 2 shall apply and the “time period” shall be thirty (30) days;

### In *Clause 11(a) – Redress*, the optional language shall not apply;

### In *Clause 13(a) – Supervision*, the following shall be inserted: the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex 1.C**, shall act as competent supervisory authority.

### In *Clause 17 – Governing law*, Option 2 shall apply and the “Member State” shall be Ireland;

### In *Clause 18 – Choice of forum and jurisdiction*, the Member State shall be Ireland;

### *Annex I* shall be deemed completed with the relevant sections of **Annex 1** to this DPA;

### *Annex II* shall be deemed completed with the relevant sections of **Annex 2** to this DPA; and

### *Annex III* shall be deemed completed with the relevant sections of **Annex 3** to this DPA.

## In respect of Restricted Transfers from the UK, the SCCs (as incorporated by reference) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is as set forth below:

## Table 1 – the Parties are ALERT and Customer, with contact details as set forth in **Annex 1** to this DPA.

## Table 2 – the Approved EU Standard Contractual Clauses with optional provisions as set forth in Section 9.2.

## Table 3 – the Annexes are deemed completed with the relevant information contained in the Annexes to this DPA.

## Table 4 – neither Party has the right of termination set forth in Section 19 of the UK IDTA.

## The parties agree that with respect to Swiss Personal Data the EU SCCs will apply amended and adapted as follows:

### the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority;

### the term “member state” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and

### references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced).

## If ALERT receives legal process requiring disclosure of Customer Personal Data to a public authority in a Third Country that does not benefit from an adequacy decision, ALERT shall promptly, and as applicable: (i) inform the relevant public authority of the incompatibility of the legal process with the safeguards provided under this DPA, and the resulting conflict of obligations for ALERT; (ii) promptly notify Customer of the legal process; (iii) assess the lawfulness of the legal process; (iv) respond to the legal process by using reasonable efforts to challenge the validity of the legal process where there are grounds to do so; (v) seek interim measures to suspend the effects of the legal process until the relevant court or authority has decided on the merits; (vi) refrain from disclosing the Customer Personal Data until required to do so under the applicable procedural rules; and (vii) provide the minimum amount of Customer Personal Data permissible when responding to the legal process, based on a reasonable interpretation thereof.

## ALERT shall inform Customer of developments that might lead to ALERT’ inability to comply with its obligations under this DPA (including the SCCs). In the event of any such change, Customer shall be entitled to immediately (i) suspend the transfer of Customer Personal Data, (ii) terminate this DPA, and/or (iii) require ALERT to return or delete the Customer Personal Data.

# Liability

## ALERT’s limitations of, and exclusions from, liability are as set forth in the Agreement; provided that ALERT shall not be liable for costs or damages incurred by Customer as a result of an action or inaction by Customer or customer’s users or clients that causes or results in a Security Incident.

# General Terms

## Precedence. To the extent there is any conflict between the Agreement, this DPA, and/or the SCCs, the various agreements will control in the following order of preference: (i) the SCCs, (ii) this DPA, (iii) the Agreement.

## Survival. Any obligation imposed on ALERT or any ALERT Affiliate under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of this DPA.

## Governing Law. This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects in accordance with the choice of law and jurisdiction clauses contained in the Agreement.

**AGREED AND ACKNOWLEDGED:**

|  |  |
| --- | --- |
| ALERTENTERPRISE, INC.  (“ALERT”)  By \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [CUSTOMER] (“Customer”)  By \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

### **ANNEX 1 – DESCRIPTION OF THE PROCESSING**

# LIST OF PARTIES

**Data exporter(s):**

|  |  |  |
| --- | --- | --- |
| 1) | Name: | [Customer] |
| Address: | [Customer Address] |
| Contact person’s name, position, and contact details: | [Customer contact] |
| Activities relevant to the data transferred under these Clauses: | Use of ALERT’s Services as described in the Agreement. |
| Role (controller/processor): | Controller |

**Data importer(s):**

|  |  |  |
| --- | --- | --- |
| 1) | Name: | ,AlertEnterprise Inc., NC. |
| Address: | 4350 Start Board Dr, Fremont, CA 94538neet JLERT ADDRESS |
| Contact person’s name, position, and contact details: | Puneet Jain  Puneet.jain@alertenterprise.com  Ae-devops@alertenterprise.com |
| Activities relevant to the data transferred under these Clauses: | P and supporting the Services as described in the Agreement. |
| Role (controller/processor): | Processor |

# DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred / processed (delete or add as necessary)*

* Customer’s employees, contractors, and contingent workers.
* Customer’s visitors.

*Categories of personal data transferred / processed (delete or add as necessary)*

* Contact information
* Identifying information
* Geolocation information
* Professional information

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

* Unless otherwise agreed, the transferred Personal Data may comprise special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person’s sex life or sexual orientation. Taking into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons, ALERT has implemented the technical and organizational measures as described in Annex II, including specialized training of staff and system access logs, to ensure an appropriate level of protection for such sensitive data.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

* Transfers will be made on (select one):
  + ☐ continuous basis.
  + ☐ a one-off basis commencing on DATE and terminating on DATE.

*Nature of the processing*

* The nature of the processing (i.e., the Services provided) is as described in the Agreement.

*Purpose(s) of the data transfer and further processing*

* To provide the Services as described in the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

* Customer Personal Data will be retained for the duration of the Agreement, after which point ALERT will delete the Customer Personal Data unless otherwise required under applicable law.

*For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing*

* The subject matter and duration of the processing is as outlined above within this Annex. The nature of the specific subprocessing services is as further described in the Subprocessor list provided by ALERT.

# COMPETENT SUPERVISORY AUTHORITY

* The competent supervisory authority is as determined in accordance with Clause 13 of the Standard Contractual Clauses.

**ANNEX 2 - TECHNICAL AND ORGANI**Z**ATIONAL MEASURES**

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons:

***ALERT shall comply with the following Information Security Requirements:***

Capitalized terms used herein have the meanings given in the DPA or the Agreement, as applicable.

ALERT shall maintain a written information security program that contains administrative, technical, and physical safeguards that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of Customer Personal Data, as well as the associated risks, are (a) appropriate to the type of information that ALERT will store; (b) appropriate to the need for security and confidentiality of such information; and (c) align with industry standards, including the International Organization for Standardization’s (ISO) standards and SOC2.

ALERT’ security program includes:

**Security Program**

ALERT shall put in place and shall maintain a comprehensive, written information security program that includes policies, procedures, and controls with administrative, technical, and physical safeguards applicable to the storage, transmission, processing and security of Customer Personal Data. ALERT shall employ physical, technical, and administrative measures that are intended to (i) protect Customer Personal Data from unauthorized access, destruction, alteration, loss, or disclosure; (ii) secure physical facilities; (iii) secure network links between offices and data centers; and (iii) protect hosted applications from unauthorized access.

**Physical Security**

*Access Security.* ALERT shall use gated and badged access security measures at all its facilities that host, or from which can be accessed, Customer Personal Data.

*Media, Systems, Machines and Devices.* ALERT shall enforce restrictive protocols for removable media and physical assets, and strives to adhere to strict data removal, storage, and destruction standards to protect data through the entire lifecycle.

ALERT shall maintain an inventory of all physical and information assets in its configuration management systems. ALERT maintains and verifies equipment containing storage media to ensure that any sensitive data and licensed software is removed or securely overwritten prior to disposal or re-use. ALERT shall require its Affiliates and Subprocessors to follow industry standard destruction of sensitive materials before disposition and destruction of hard disk drives containing Customer Personal Data.

**Technical Security**

*Network Security****.***  ALERT shall employ security measures intended to protect data from unauthorized access, including redundant firewalls with intrusion detection systems and intrusion protection systems.

*Encryption****.***ALERT shall employ encryption measures intended to protect Customer Personal Data using current industry-standard algorithms and key lengths.

*Access control.* ALERT shall maintain a Role-based Access Control (RBAC) system that is intended to restrict network access based on the roles of individuals users.

*MFA.* ALERT strives to enforce multi-factor authentication (MFA) where available, and shall have in place password strength and complexity requirements for all users.

*MDM.* ALERT shall implement mobile device management controls intended to protect Customer Personal Data when accessed on mobile devices.

*Change Management.* ALERT shall employ a change management system to help ensure that changes to the organization, business processes, information processing facilities, and systems that affect information security, privacy, and availability are controlled. ALERT shall maintain a configuration management system that inventories devices, installs software, prevents the installation of blacklisted software, installs certificates, applies security configurations, and applies security and other Microsoft and third party patches.

**Administrative Security**

*Personnel and Contractor Security.*  ALERT shall conduct background verification checks for its personnel proportional to the business requirements, the classification of the information to be accessed, and the perceived security risks associated with a position.

ALERT shall enter into NDAs and confidentiality agreements with employees, contractors, Subprocessors, and Third Parties, each of whom access systems and services only on a need-to-know basis*.* ALERT endeavors to ensure that critical vendors have recognized third party security certifications.

ALERT shall provide security and privacy awareness training to employees of ALERT and, where appropriate, as relevant to their job function.

*Accountability.* ALERT shall implement organizational requirements under the accountability principle, including compliance with applicable Data Protection Laws through a strong culture of compliance, accountability for compliance with the data security protocols including establishment, documentation and maintenance of business processes and controls.

**Testing and Evaluating Security Measures**

ALERT shall perform vulnerability identification and penetration tests and assessments against its systems that Process Customer Personal Data. ALERT performs risk assessments of the physical and logical security measures and safeguards it maintains.

ALERT shall maintain a vulnerability management system that scans internal systems, external systems and web applications for known vulnerabilities. ALERT periodically engages third parties to review its security controls.

**Incident Management.**

ALERT shall employ an incident management plan that establishes management responsibilities and procedures documenting the necessary steps and channels of communication to be followed when responding to Security Incidents.

**Restoration and Access after a Physical or Technical Incident**

ALERT shall maintain a business continuity plan and a disaster recovery plan intended to prevent Customer Personal Data loss and to maintain ALERT’s delivery of its services with minimal interruption. ALERT tests and updates its disaster recovery and business continuity plans.

ALERT shall implement redundant logical and physical assets where needed to meet availability requirements.

ALERT shall test backup copies of information, software, and system images in accordance with its backup policy.

**System configuration, planning and management**

ALERT shall maintain processes and procedures for effective management of its systems and their configuration.

**Certifications**

Where relevant, ALERT shall align its controls with industry recognized standards and obtain certifications if needed.

**Customer Responsibilities**

Customer shall (i) ensure that Customer’s approved users follow the same terms of service that apply to Customer; (ii) secure computer systems or devices in Customer’s possession, custody, or control from threats that might impact the security, confidentiality, availability, and privacy of data; (iii) if Customer directs the use of data transfer tools or methods, Customer shall be responsible for securing the portion of the chain of custody that Customer controls, including any onward transfers Customer directs which are outside the control of ALERT; (iv) direct the transfer of data between jurisdictions, including to approve or deny EU country to EU country data replication for disaster recovery and business continuity; (v)protect the confidentiality of each Customer user’s login and password and managing each Customer user’s access to the Services, and prohibiting the sharing of accounts and/or passwords; (vi) take appropriate action to secure, protect, and backup Customer Data in a manner that will provide appropriate security and protection, including encryption to protect Customer Data; and (vii) employ best practices to prevent uploading data containing malicious code into ALERT’s systems.

**Subprocessors**

ALERT contractually requires its Subprocessors take the same or substantially similar measures described in this Annex 2. Subprocessors are found on our Subprocess List available in Annex 3.

### **ANNEX 3 - SUBPROCESSORS**

The controller has authorized the use of the Subprocessors found in its Subprocessor List available below:

|  |  |  |  |
| --- | --- | --- | --- |
| Subprocessor Name: | Address: | Data Storage Location: | Description of Processing: |
| AWS | Seattle, WA (USA) | Seattle, WA (USA)  EUROPE | Customers Employee Information storage and Processing for security use cases. |
| HID | Austin, TX (USA) | Austin, TX (USA) | Customer Employee PII who use mobile credentials. |
| Wavelynx | Broomfield, CO | Broomfield, CO (USA) | Customer Employee PII who use mobile credentials. |
| SafeTrust | Fremont, CA | Fremont, CA (USA) | Customer Employee PII who use mobile credentials. |
| Microsoft Azure | Seattle, WA (USA) | Seattle, WA, (USA) | Customers Employee Information storage and Processing for security use cases. |