INTEGSEC

https://integsec.com/
+1 207-200-3288
legal@integsec.com
PO Box 372, Bethel, ME 04217

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") is entered into as of the Effective Date set forth below, by and between:

Effective Date: [Document.CreatedDate]

IntegSec LLC (and its affiliates), with registered address at 5305 Limestone Rd Suite 200, Wilmington, DE 19808 ("IntegSec" or the "Processor"), and

Controller Name: [Client.Company]

Registered Address: [Client.StreetAddress], [Client.City], [Client.State] [Client.PostalCode]

(the "Controller").

1. Scope and Purpose

1.1 This DPA applies to the processing of Personal Data by IntegSec on behalf of the Controller in connection with the services provided under the Master Service Agreement, Subscription Agreement, or other service agreement between the Parties (the "Service Agreement").

1.2 This DPA is incorporated into and forms part of the Service Agreement. In the event of a conflict between this DPA and the Service Agreement, this DPA shall prevail with respect to the processing of Personal Data.

2. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person that is processed by IntegSec on behalf of the Controller in connection with the Service Agreement.

"Processing" means any operation performed on Personal Data, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.

"Data Protection Laws" means all applicable laws relating to the processing of Personal Data, including the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and any other applicable data protection legislation.

"Security Incident" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

3. Processing Instructions

3.1 IntegSec will process Personal Data only on documented instructions from the Controller, including with respect to transfers of Personal Data to a third country, unless required to do so by applicable law. In such a case, IntegSec will inform the Controller of that legal requirement before processing, unless prohibited by law.

3.2 The details of processing (subject matter, duration, nature, purpose, types of Personal Data, and categories of data subjects) are described in Annex 1 to this DPA.

4. Confidentiality

IntegSec will ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Security Measures

5.1 IntegSec will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate: (a) encryption of Personal Data at rest and in transit; (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures.

5.2 IntegSec will not access, store, or exfiltrate actual production Personal Data encountered during security testing, unless explicitly authorized in the applicable Rules of Engagement. Screenshots used as evidence will redact Personal Data where feasible.

6. Sub-processors

6.1 The Controller grants IntegSec general written authorization to engage sub-processors. IntegSec will inform the Controller of any intended changes concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object to such changes within fifteen (15) days of notification.

6.2 Where IntegSec engages a sub-processor, IntegSec will impose on the sub-processor the same data protection obligations as set out in this DPA by way of a contract. IntegSec remains fully liable to the Controller for the performance of the sub-processor's obligations. IntegSec's liability under this Section 6.2 is subject to the limitation of liability provisions in the Service Agreement.

6.3 If the Controller objects to a new Sub-processor on reasonable data protection grounds, IntegSec will use commercially reasonable efforts to provide an alternative arrangement or address the Controller's concerns. If the Parties cannot resolve the objection within thirty (30) days, the Controller may terminate this DPA and the affected Services without penalty by providing written notice.

7. Data Subject Rights

7.1 IntegSec will assist the Controller, by appropriate technical and organizational measures and insofar as possible, in fulfilling the Controller's obligation to respond to requests from data subjects exercising their rights under Data Protection Laws.

7.2 IntegSec will respond to Controller requests for assistance with data subject rights within ten (10) business days of receipt, or such shorter period as required by Data Protection Laws.

8. Data Protection Impact Assessments and Consultation

8.1 IntegSec will assist the Controller, taking into account the nature of processing and the information available to IntegSec, in ensuring compliance with the Controller's obligations under Articles 35 and 36 of the GDPR (or equivalent provisions under other Data Protection Laws) with respect to data protection impact assessments and prior consultation with supervisory authorities.

9. Records of Processing Activities

IntegSec will maintain records of all categories of processing activities carried out on behalf of the Controller in accordance with Article 30(2) of the GDPR (or equivalent provisions under other Data Protection Laws). Such records will be made available to the Controller and any supervisory authority upon request.

10. CCPA Compliance

10.1 To the extent the CCPA applies, IntegSec is a "service provider" as defined under the CCPA and will not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than performing the Services specified in the Service Agreement; or (c) retain, use, or disclose Personal Data outside of the direct business relationship between IntegSec and the Controller, except as permitted by the CCPA; or (d) not combine Personal Data received from or on behalf of the Controller with personal data received from any other source, except as expressly permitted by the CCPA.

10.2 IntegSec certifies that it understands and will comply with the restrictions set forth in this Section 10.

11. Security Incident Notification

11.1 IntegSec will notify the Controller without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Security Incident affecting Personal Data processed under this DPA.

11.2 The notification will include: (a) a description of the nature of the Security Incident; (b) the categories and approximate number of data subjects and records concerned; (c) the likely consequences of the incident; and (d) the measures taken or proposed to address the incident.

12. Data Deletion and Return

Upon termination of the Service Agreement, IntegSec will, at the Controller's choice, delete or return all Personal Data within thirty (30) days and delete existing copies, unless applicable law or the data retention period in the Service Agreement (e.g., eighteen (18) months for final reports) requires continued storage.

IntegSec will provide written certification of deletion upon request. Continued retention of final reports during the retention period is justified under GDPR Article 17(3)(e) for the establishment, exercise, or defense of legal claims and compliance with professional standards.

13. Audit Rights

13.1 IntegSec will make available to the Controller all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

13.2 Audits will be conducted with reasonable advance notice (not less than 30 days), during normal business hours, and no more than once per calendar year unless required by a supervisory authority or following a Security Incident.

14. International Transfers

14.1 IntegSec will not transfer Personal Data to a country outside the European Economic Area (EEA) or the United Kingdom unless appropriate safeguards are in place as required by Data Protection Laws, such as Standard Contractual Clauses approved by the European Commission, the UK International Data Transfer Agreement, or an adequacy decision.

14.2 Where the Standard Contractual Clauses approved by European Commission Implementing Decision (EU) 2021/914, as amended or replaced from time to time, or an International Data Transfer Agreement are required, the Parties will execute such clauses as a separate addendum to this DPA, which shall be incorporated by reference.

14.3 IntegSec will cooperate with the Controller in conducting Transfer Impact Assessments where required and will implement supplementary technical and organizational measures where a Transfer Impact Assessment identifies risks to data subjects.

15. Sub-processor List

15.1 IntegSec will maintain a current list of Sub-processors and will provide this list to the Controller upon execution of this DPA and upon request thereafter. The list will include the sub-processor's name, location, and a description of the processing activities performed.

15.2 IntegSec will notify the Controller in writing at least fifteen (15) days prior to engaging any new sub-processor or replacing an existing sub-processor. The Controller may object to the change in accordance with Section 6.

16. Term

This DPA shall remain in effect for the duration of the Service Agreement and shall automatically terminate upon termination of the Service Agreement, subject to the data deletion obligations in Section 12.

17. Limitation of Liability

17.1 IntegSec's liability under this DPA is subject to the limitation of liability provisions in the Service Agreement. In the event no Service Agreement is in effect between the Parties, each Party's total liability under this DPA shall not exceed $100,000 or the total fees paid or payable between the Parties in the twelve (12) months preceding the claim, whichever is greater.

17.2 Neither Party is liable for indirect, consequential, punitive, or special damages (including lost profits) arising under this DPA, even if advised of the possibility. Exceptions: fraud and willful misconduct.

17.3 The liability caps in this DPA and the Service Agreement are not cumulative. The total combined liability of either Party across this DPA, the Service Agreement, and any related Statements of Work or Subscription Agreements for all claims arising from the same facts or circumstances shall not exceed the higher of the applicable caps under those agreements.

18. Governing Law and Dispute Resolution

18.1 This DPA is governed by the same governing law as the Service Agreement, except where Data Protection Laws require otherwise. If no Service Agreement is in effect, this DPA is governed by the laws of the State of Delaware.

18.2 Any dispute arising out of or in connection with this DPA shall be resolved in accordance with the dispute resolution provisions of the Service Agreement. If no Service Agreement is in effect, disputes shall be resolved by binding arbitration under the Commercial Arbitration Rules of the American Arbitration Association (AAA), administered in Wilmington, Delaware. The prevailing Party recovers reasonable attorneys' fees and costs.

18.3 JURY TRIAL WAIVER: EACH PARTY IRREVOCABLY WAIVES THE RIGHT TO TRIAL BY JURY IN ANY ACTION, PROCEEDING, OR COUNTERCLAIM ARISING OUT OF OR RELATING TO THIS DPA.

18.4 Limitation Period: Any claim arising under or related to this DPA must be commenced within two (2) years after the claimant knew or reasonably should have known of the facts giving rise to the claim, regardless of the form of action.

18.5 Anti-Assignment of Claims: Neither Party may assign, transfer, or delegate any claims, causes of action, or rights to recover damages arising under this DPA to any third party without the other Party's prior written consent.

18.6 Severability: If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall continue in full force and effect.

18.7 Entire Agreement: This DPA, together with the Service Agreement, constitutes the entire agreement between the Parties regarding the processing of Personal Data. Amendments to this DPA must be in writing and signed by both Parties.

18.8 Assignment: Neither Party may assign this DPA without the other Party's prior written consent, except that IntegSec may assign this DPA in connection with a merger, acquisition, or sale of substantially all of its assets, provided the assignee agrees to be bound by the terms of this DPA.

18.9 Notices: All notices under this DPA shall be in writing and sent to the addresses specified in this DPA or the Service Agreement.

18.10 Force Majeure: Neither Party shall be liable for delays or failures in performing its obligations under this DPA due to events beyond reasonable control, provided that the affected Party promptly notifies the other Party and uses commercially reasonable efforts to resume performance.

ANNEX 1: DETAILS OF PROCESSING

Subject Matter of Processing: Processing of Personal Data as necessary for IntegSec to perform cybersecurity assessment services under the Service Agreement.

Duration of Processing: For the term of the Service Agreement plus any retention period specified therein.

Nature and Purpose of Processing: Security testing, vulnerability assessment, and related cybersecurity services. Processing is limited to incidental encounters with Personal Data during authorized testing activities.

Types of Personal Data: Any Personal Data that may be incidentally encountered during security testing of in-scope systems, which may include names, email addresses, IP addresses, credentials, and other data stored on or transmitted through the systems under test.

Categories of Data Subjects: Employees, contractors, customers, and other individuals whose Personal Data may be stored on or transmitted through the systems under test.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

IntegSec LLC

By: _____

Name: Michel Chamberland

Title: Founder and CEO

Controller

By: _____

Name: [Client.FirstName] [Client.LastName]

Title: [Client.Title]

Email: [Client.Email]

Company: [Client.Company]