IDVerifact Technologies, Inc.,
Data Processing Addendum (V. 20211123)

This Data Processing Addendum ("**DPA**"), forms part of the SOFTWARE AS A SERVICE AGREEMENT (hereafter referred to as "**Agreement**") between IDVerifact Inc. ("**IDVerifact**") and Customer and shall be effective as of the effective date of the Agreement ("**Effective Date**").

1. Definitions

1.1 The following terms shall have meanings ascribed for the purposes of this DPA:

"**Affiliate**" meansan entity that controls, is controlled by or shares common control with a party, where such control arises from either (i) a direct or indirect ownership interest of more than 50% or (ii) thepower to direct or cause the direction of the management and policies, whether through the ownership of voting stock by contract, or otherwise, equal to that provided by direct or indirectownership of more than 50%.

"**Agreement**" has the meaning ascribed to such term in the first paragraph of this agreement.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Information under the Agreement.

"**Personal Information**" means any information (i) relating to an identified or identifiable natural person; or (ii) defined as "personally identifiable information", "personal information", "personal data" or similar terms, as such terms are defined under Data Protection Laws.

"**Process**", "**Processes**", "**Processing**", and "**Processed**" means any operation or set of operations performed upon Customer Personal Data whether or not by automatic means.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data on systems managed by or otherwise controlled by IDVerifact.

"**Services**" means the services provided by IDVerifact to Customer pursuant to the Agreement, which may include: (i) support and maintenance services for its on-premises Software; (ii) SaaS Services; and (iii) professional services (e.g. implementation services, expert services, and training services) provided by IDVerifact to Customer pursuant to the Agreement.

"**Sub-processor**" means any entity engaged by IDVerifact or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

Sub-processors may include third parties or IDVerifact's affiliates. Sub-processors may also include subcontractors that are specified in an applicable Statement of Works.

1.2 Capitalized terms used in this DPA that are not defined in this DPA shall havethe meaning ascribed to them in the Agreement.

2. Jurisdiction-Specific Addenda

2.1 Attached to this DPA are Addenda that provide terms specific to the Processing of Customer Personal Information arising out of specific legal requirements from particular jurisdictions. In the event that Customer Personal Information is Processed from one or more of these jurisdictions, and the applicable requirements are not already covered in this DPA, then the terms in the respective Addendum attached hereto shall apply.

2.2 In the event of a conflict between the Agreement or this DPA and an Addendum, the Addendum applicable to Customer Personal Information from the relevant jurisdiction shall control with respect to Customer Personal Information from that relevant jurisdiction, and solely with regard to the portion of the provision in conflict.

2.3 Customer has sole responsibility for informing IDVerifact when Customer Personal Information is within the scope of one or more Addenda. Customer confirms that, at the time of execution of this DPA, Customer Personal Information is within the scope of the following Addenda:

☐ California Consumer Privacy Act Addendum

2.4 In the event, Customer believes additional Addenda should apply, Customer has the sole responsibility for notifying IDVerifact and working with IDVerifact to effectuate such Addenda.

3. Updates to DPA

3.1 In the event of changes to applicable Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, the parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Addenda.

4. Roles and Scope of Processing

4.1 **Customer Processing of Personal Information**. Customer agrees that: (i) it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Information and any Processing instructions it issues to IDVerifact; and (ii) it has provided all fair processing notices and obtained all consents and rights necessary under Data Protection Laws for IDVerifact to Process Personal Information and provide the Services pursuant to the Agreement and this DPA.

4.2 **Customer Instructions**. IDVerifact will Process Customer Personal Information only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions and applicable Data Protection Laws. IDVerifact will not Process Customer Personal Information provided by or collected on behalf of Customer for any purpose except as necessary to maintain or provide the Services specified in the Agreement and this DPA, oras necessary to comply with the law or binding order of a governmental body. In the event thatIDVerifact has a legal obligation to Process the Customer Personal Information, IDVerifact will notify the Customer of this obligation unless it is legally prohibited from doing so. The parties agree that this DPA, including all applicable Addenda, and the Agreement set out the Customer's complete instructions to IDVerifact in relation to the Processing of Customer Personal Information by IDVerifact. Additional Processing outside the scope of these instructions (if any) will require a prior written agreement between Customer and IDVerifact.

4.3 **Details of Data Processing.**

(a) Categories of data subjects whose Personal Information is transferred

Customer's employees, contractors, and/or business partners and/or end-users authorized by Customer. Customer's customers' personal and organizational.

(b) Categories of Personal Information transferred

Identification and contact data (e.g., name, address, title, contact details), employment details (e.g., job title, role, manager), and/or IT information (e.g., entitlements, IP addresses, usage data, cookies data, and geolocation).

(c) Sensitive data transferred (if applicable)

Customer's customers' Personal Information.

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

For support and maintenance and professional services: one-off. Customer controls what information (including Personal Information) it shares with IDVerifact and when it shares such information (including Personal Information) in the context of the provision of ancillary support and account administration services under the Agreement.

For SaaS Services: continuous. Customer controls what information (including Personal Information) it shares with IDVerifact and what systems it connects to the SaaS Services. The SaaS Services may allow for a one-off data transfer or connectivity to facilitate transfer on a regularly scheduled and/or continuous basis. Customer determines its configuration and use of the SaaS Services under the Agreement.

(e) Nature of the processing

To provide IDVerifact's solutions and other Services under the Agreement.

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

The provision of Services by IDVerifact under the Agreement.

(g) The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period

The Customer Personal Information Processed by IDVerifact will be retained for the duration of the Processing by IDVerifact in the context of the provision of Services under the Agreement, and thereafter in accordance with the Agreement and in order to comply with applicable law, includingData Protection Laws.

5. Sub-processing

5.1 **Authorized Sub-processors**. Customer agrees that IDVerifact may engage Sub-processors to Process Customer Personal Information on Customer's behalf.

5.2 **Sub-processor Obligations**. IDVerifact will: (i) not engage a Sub-processor unless IDVerifact enters into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Information to the same standard as IDVerifact; and (ii) remain responsible for its compliance with the obligations of this DPA and for any failure by a Sub-processor engaged by IDVerifact to fulfil its data protection obligations under the applicable Data Protection Laws.

6. Security

6.1 **Security Measures**. Taking into account the nature of the Processing, IDVerifact shall implement and maintain reasonable technical and organizational security measures to protect Customer Personal Information from Security Incidents and to preserve the security and confidentiality of the Customer Personal Information, in accordance with IDVerifact's security standards described in **Annex A**, as applicable to the Services ("**Security Measures**").

6.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by IDVerifact relating to the Security Measures and making an independent determination as to whether such Security Measures meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that IDVerifact may update or modify the Security Measures from time-to-time provided that such updates and modifications do not result in a material degradation of the overall security of the Services.

6.3 **Customer Responsibilities**. Customer agrees that, without prejudice to IDVerifact's obligations under Section 6.1 (Security Measures) and Section 9.2 (Security Incident Response):

(a) Customer is responsible for its use of the Services, including: (i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Information;(ii) securing its account authentication credentials; (iii) protecting the security of Customer Personal Information when in transit to and from the Services; (iv) taking appropriate steps to securely encrypt and/or backup any Customer Personal Information uploaded to the Services; and (v) properly configuring the Services and using available features and functionalities to maintain appropriate security in light of the nature of the Customer Personal Information Processed as a result of Customer's use of the Services; and

(b) IDVerifact has no obligation to protect Customer Personal Information that Customer elects to store or transfer outside of IDVerifact's and its Sub-processors' (where applicable) systems (for example, offline or on-premises storage).

7. Security Reports and Audits

7.1 Upon request, IDVerifact shall provide to Customer (on a confidential basis) a summary copy of any third-party audit report(s) or certifications applicable to the Services ("**Report**"), so that Customer can verify IDVerifact's compliance with this DPA, the audit standards against which it has been assessed, and the standards specified in the IDVerifact Security Measures, as described in **Annex A**.

7.2 If Customer reasonably believes that the Report provided is insufficient to demonstrate compliance with this DPA, IDVerifact shall also provide written responses (on a confidential basis) to reasonable requests for information made by Customer related to its Processing of Customer Personal Information, including responses to information security and audit questionnaires that are reasonably necessary to demonstrate IDVerifact's compliance with this DPA, provided that Customer shall not be permitted to exercise this right more than once every 12 months.

7.3 If Customer reasonably believes that the information provided pursuant to Sections 7.1 and/or 7.2 is insufficient to demonstrate compliance with this DPA, IDVerifact will allow an audit by Customer (or auditors appointed by Customer and reasonably acceptable to IDVerifact) in relation to IDVerifact's Processing of Customer Personal Information. Any such audit will be at Customer's expense, with reasonable advance notice, conducted during normal business hours, carried out no more than once every 12 months and subject to IDVerifact's reasonable

security and confidentiality requirements, provided that the exercise of rights under this Section would not infringe Data Protection Laws.

8. International Operations

8.1 In the event that IDVerifact is providing SaaS Services to the Customer, any Customer Data that the Customer uploads to the SaaS Services shall remain at all times at the location of the host (as detailed in the Agreement). With respect to its general provision of the Services, IDVerifact may store and Process Customer Personal Information in IDVerifact's internal systems anywhere in the world where IDVerifact, its Affiliates or its Sub-processors maintain data processing operations.

9. Additional Security

9.1 **Confidentiality of Processing**. IDVerifact shall ensure that any person who is authorized by IDVerifact to Process Customer Personal Information (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2 **Security Incident Response**. IDVerifact shall: (i) taking into account the nature of IDVerifact's Processing of Customer Personal Information and the information available to IDVerifact, notify Customer of a Security Incident that it becomes aware of, without undue delay; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.3 **Notification**. Customer acknowledges that IDVerifact will not assess the contents of Customer Personal Information in order to identify information subject to any specific legal requirements. Customer is solely responsible to comply with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incidents as required by Data Protection Laws. Unless otherwise required under Data Protection Laws, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory authorities.

10. Relationship with the Agreement

10.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Information.

10.2 Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by IDVerifact that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce IDVerifact's liability under the Agreement as if it were liability to the Customer under the Agreement.

10.3 Any claims against IDVerifact or its Affiliates under this DPA shall only be brought by the Customer that is a party to the Agreement against IDVerifact. In no event shall this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

10.4 This DPA will be governed by and construed in accordance with governing law and jurisdiction

provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

10.5 This DPA will terminate automatically with the termination or expiry of the Agreement, subject to additional provisions in any Addenda attached hereto.

10.6 For purposes of interpreting this DPA, (a) unless the context otherwise requires, the singular includes the plural, and the plural includes the singular; (b) unless otherwise specifically stated, the words “herein,” “hereof,” and “hereunder” and other words of similar import refer to this DPA as a whole and not to any particular section or paragraph; (c) the words “include” and “including” will not be construed as terms of limitation, and will therefore mean “including but not limited to” and “including without limitation”; (d) unless otherwise specifically stated, the words “writing” or “written” mean preserved or presented in retrievable or reproducible form, whether electronic (including email but excluding voice mail) or hard copy; and (e) the captions and section and paragraph headings used in this DPA are inserted for convenience only and will not affect the meaning or interpretation of this DPA. This DPA may be executed in one or more counterparts, either in original, facsimile or scanned electronic form, each of which so executed shall constitute an original and all of which together shall constitute one and the same agreement.

Company: _____

Signature: _____

Name: _____

Title: _____

Date Signed: _____

Company: IDVerifact Inc.

Signature: _____

Name: Tom Beckerman

Title: CEO

Date Signed:

.Annex A – Security Measures

IDVerifact Data Security

Program

IDVerifact has implemented and shall maintain a commercially reasonable security program in accordance with industry best practices, which shall include technical and organizational measures to ensure an appropriate level of security for Customer Personal Data taking into account the risks presentedby the processing, in particular from the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to Customer Personal Data, and the nature of the Customer Personal Data to be protected having regard to the state of the art and the cost of implementation. IDVerifact's security programshall include the following measures.

1. Security Program

a. ISO27001-based Information Security Management System (ISMS): IDVerifact shall maintain an ISMS risk-based security program to systematically manage and protect the organization'sbusiness information and the information of its customers and partners.
b. Security Governance Committee: IDVerifact shall maintain a security committee comprised of executive and senior leaders that oversee the company's security program. This committee shall meet monthly to review the operational status of the ISMS (including risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.
c. Security incident response policy: IDVerifact shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorizations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.
d. Policy maintenance: All security and privacy-related policies shall be documented, reviewed, updated, and approved by management at least annually to ensure they remain consistent withbest practices, legal and regulatory requirements, and industry standards.
e. Communication and commitment: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant subcontractors. Securityshall be addressed at the highest levels of the company with executive management regularlydiscussing security issues and leading company-wide security initiatives.

2. Personnel Security

a. Background screening: Personnel who have access to Customer Personal Data or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations) that shall include verification of identity, right to work and academic degrees and a check of criminal records, sex offender registries and prohibited/denied party lists.
b. Confidentiality obligations: Personnel who have access to Customer Personal Data shall be subject to a binding contractual obligation with IDVerifact to keep the Customer Personal Data confidential.
c. Security awareness training: Personnel shall receive training upon hire and at least annually thereafter covering security best practices and privacy principles.
d. Code of conduct: IDVerifact shall maintain a code of business conduct policy and

compliance program to ensure ethical behaviour and compliance with applicable laws and regulations.

3. Third-Party Security

a. Screening: IDVerifact shall maintain policies and procedures to ensure that all new suppliers, SaaS applications, IT Software, and IT service solutions are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

b. Contractual obligations: IDVerifact shall ensure that contractual agreements with suppliers include confidentiality and privacy provisions as appropriate to protect IDVerifact's interests andto ensure IDVerifact can meet its security and privacy obligations to customers, partners, employees, regulators, and other stakeholders.

c. Monitoring: IDVerifact shall periodically review existing third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements. The monitoring program shall review suppliers at least annually (regardless of the length of contractual term) to confirm that the supplier/solution is still meeting the company's objectivesand the supplier's performance, security, and compliance postures are still appropriate given the type of access and classification of data being accessed, controls necessary to protect data, and applicable legal and regulatory requirements.

4. Physical Security

a. Corporate facility security: A facility security program shall be maintained that manages building entrances, CCTVs, and overall security of its offices, including a security perimeter (including barriers such as card controller entry gates or manned reception desks). All employees, contractors and visitors shall be required to wear identification badges that distinguish their respective roles.

b. SaaS Services data center security: IDVerifact leverages Infrastructure as a Service (IaaS) datacenters for hosting the SaaS Services. IDVerifact assesses the security and compliance measures of the applicable data center providers, and the providers follow industry best practices and comply with numerous standards.

5. Solution Security

a. Software development life cycle (SDLC): IDVerifact shall maintain a software development life cycle policy that defines the process by which personnel create secure products and servicesand the activities that personnel must perform at various stages of development (requirements, design, implementation, verification, documentation, and delivery).

b. Secure development: Product management, development, test, and deployment teams shall follow secure application development policies and procedures that are aligned to industry-standard practices.

c. Vulnerability assessment: IDVerifact shall regularly conduct risk assessments, vulnerability scans and audits (including third-party penetration testing of the SaaS Services twice annuallyand software upon each new version release). Identified product solution issues shall be scored using the Common Vulnerability Scoring System (CVSS) risk-scoring methodology based on risk impact level and the likelihood and potential consequences of an issue occurring. Vulnerabilities are remediated based on assessed risk. Upon request from Customer, IDVerifact shall provide information about the identified vulnerabilities and

the measures taken to remediate or address any such vulnerabilities.

6. Operational Security

a. Access controls: IDVerifact shall maintain policies, procedures, and logical controls to establishaccess authorizations for employees and third parties to limit access to properly authorized personnel and to prevent unauthorized access. Such controls shall include:
   i. requiring unique user IDs to identify any user who accesses systems or data.
   ii. managing privileged access credentials in a privileged account management (PAM)system.
   iii. communicating passwords separately from user IDs.
   iv. ensuring that user passwords are (1) changed at regular intervals; (2) of sufficient length and complexity; (3) stored in an encrypted format; (4) subject to reuse limitations; and (5) not assigned to other users, even at a different time; and
   v. automatically locking out users' IDs when several erroneous passwords have been entered.

b. Least privilege: IDVerifact shall ensure that personnel only have access to systems and data asrequired for the performance of their roles; only authorized personnel have physical access to infrastructure and equipment; access to production resources for the SaaS Services is restricted to employees requiring access, and access rights are reviewed and certified at leastannually to ensure access is appropriate.

c. Malware: IDVerifact shall utilize industry-standard measures to detect and remediate malware,viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorized access to information or systems.

d. Encryption: IDVerifact shall use industry-standard strong encryption methods to protect data intransit and at rest as appropriate to the sensitivity of the data and the risks associated with loss;all laptops and other removable media, including backup tapes, on which Customer Personal Data is stored shall be encrypted.

e. Business continuity and disaster recovery (BCDR): IDVerifact shall maintain formal BCDR plansthat are regularly reviewed and updated to ensure IDVerifact's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. Data backups: IDVerifact shall backup data and systems using alternative site storage availablefor restore in case of failure of the primary system. All backups shall use strong encryption in transit and at rest.

g. Change management: IDVerifact shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to IDVerifact's SaaS Services infrastructure, systems, networks, and applications.

h. Network security: IDVerifact shall implement industry-standard technologies and controls to protect network security, including firewalls, intrusion prevention systems, monitoring, network segmentation, VPN and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controlsshall be reviewed at least annually.

i. Data segregation: IDVerifact shall implement logical controls, including logical separation, access controls and encryption, to segregate Customer's Personal Information from other Customer and IDVerifact data in the SaaS Services. IDVerifact shall additionally ensure that production and non-production data and systems are separated.

California Consumer Privacy Act Addendum

1. Scope

This Addendum shall apply in the event that IDVerifact Processes Customer Personal Information of California residents.

2. Definitions

2.1 The California Consumer Privacy Act ("**CCPA**") is Cal. Civ. Code § 1798.100, et seq., as may be amended from time-to-time, and any accompanying legally binding regulations that are promulgated to address provisions in the law.

2.2 All words or phrases used herein not defined in the DPA will have the meaning assigned to them in the CCPA.

3. Terms

3.1 IDVerifact will not sell any Customer Personal Information received from Customer.

3.2 IDVerifact will not disclose Customer Personal Information to another business, person, or third party, except for the purpose of maintaining or providing the Services specified in the Agreement, including to provide Personal Information to advisers or Sub-processors as described below, or to the extent such disclosure is required by law.

4. Cooperation

4.1 Taking into account the nature of the Processing, IDVerifact shall (at Customer's request and expense) provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights under Data Protection Laws or applicable regulatory authorities relating to the Processing of Customer Personal Information under the Agreement. In the event that any request from data subjects or applicable regulatoryauthorities is made directly to IDVerifact, IDVerifact shall not respond to such communication directly without Customer's prior authorization other than to inform the requestor that IDVerifactis not authorized to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to do so, and instead, after being notified by IDVerifact, Customer shall respond. If IDVerifact is required to respond to such a request, IDVerifact will promptly notify Customer and provide it with a copy of the request unlesslegally prohibited from doing so.

4.2 If a law enforcement agency sends IDVerifact a demand for Customer Personal Information (e.g., a subpoena or court order), IDVerifact will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, IDVerifact may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Information to a law enforcement agency, then IDVerifact will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent IDVerifact is legally permitted to do so.

Company: _____	Company: IDVerifact
Signature: _____	Signature: _____
Name: _____	Name: Tom Beckerman
Title: _____	Title: CEO
Date Signed: _____	Date Signed: _____