DATA PROCESSING ADDENDUM ("DPA") VERSION 1 - INTELLICENE AS CUSTOMER'S PROCESSOR

This DPA forms part of the **ORDER/ PROPOSAL/ SALE AGREEMENT** ("**Agreement**") between: (1) the applicable Intellicene contracting entity, as specified in the Agreement or any other wholly owned subsidiary of Intellicene ("**Intellicene**") acting on its own behalf and as agent for each Intellicene Affiliate; and (2) **the customer engaging with Intellicene under the Agreement** ("**Customer**") acting on its own behalf as agent for each Customer Affiliate (each being a "**Party**" and together "**the Parties**").

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 Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

DPA table of contents:

1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Adequacy Decision**" means, for a jurisdiction with Privacy Laws that have data transfer restrictions, a country that the Supervisory Authority or other body in such jurisdiction recognises as providing an adequate level of data protection as required by such jurisdiction's Privacy Laws such that transfer to that country shall be permitted without additional requirements;

1.1.2 "**Affiliate**" means any entity which now or in the future controls, is controlled by, or is under common control with the signatory to this DPA, with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through the ownership of voting securities, by contract, or otherwise;

1.1.3 "**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, and in the context of this DPA shall mean the Customer;

1.1.4 "**Data Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller, and in the context of this DPA shall mean Intellicene;

1.1.5 "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates;

1.1.6 "**Personal Data**" shall have the meaning set out in, and will be interpreted in accordance with Privacy Laws, and in the context of this DPA, shall mean the personal data in Customer Data, Processed by Intellicene in accordance with the Services as outlined in Annex 1, which relates to a Data Subject;

1.1.7 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

1.1.8 "**Privacy Laws**" means national, federal, union, state and other laws, as applicable to Personal Data in the context and jurisdiction of the Processing, concerning the regulation of the collection, retention, processing, data security, disclosure, trans-border data flows, use of web-site cookies, email communications, use of IP addresses and meta-data collection;

1.1.9 "**Process**" or "**Processing**" means any operation or set of operations that is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, as described in Annex 1;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Personal Data from Customer to Intellicene; or

1.1.10.2 an onward transfer of Personal Data from Intellicene to a Subprocessor,

in each case, where such transfer outside of jurisdiction of Customer would be prohibited by Privacy Laws in the absence of an approved method of transfer, including through (a) an Adequacy Decision, (b) Standard Contractual Clauses, or (c) by the terms of other recognised forms of data transfer agreements or processes;

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Intellicene for Customer pursuant to the Agreement;

1.1.12 "**Standard Contractual Clauses**" means the contractual clauses approved by a Supervisory Authority pursuant to Privacy Laws which provides for multi-jurisdictional transfer of Personal Data from one jurisdiction to another where such transfer would otherwise be a Restricted Transfer;

1.1.13 "**Subprocessor**" means any third party (including any third party and any Intellicene Affiliate) appointed by or on behalf of Intellicene to undertake Processing in connection with the Services; and

1.1.14 "**Supervisory Authority**" means an independent public authority which is established in a jurisdiction under Privacy Laws with competence in matters pertaining to data protection.

1.2 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

1.3 References in this DPA to Intellicene include to Intellicene Affiliates where such Intellicene Affiliates are Subprocessors.

1.4 The terms used in this DPA shall have the meanings set forth in this DPA provided that capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain unchanged and in full force and effect.

2. Processing of Personal Data

2.1 Intellicene will not:

2.1.1 Process Personal Data other than on Customer's documented instructions (set out in this DPA and in the Agreement) unless Processing is required by a Supervisory Authority; or

2.1.2 sell Personal Data received from Customer or obtained in connection with the provision of the Services to Customer.

2.2 Customer on behalf of itself and each Customer Affiliate:

2.2.1 instructs Intellicene:

2.2.1.1 to Process Personal Data; and

2.2.1.2 in particular, transfer Personal Data to any country or territory;

in each case as reasonably necessary for the provision of the Services and consistent with this DPA.

2.3 Annex 1 sets out the subject matter and other details regarding the Processing of the Personal Data contemplated as part of the Services.

3. Intellicene Personnel

Intellicene shall ensure that persons authorised to undertake Processing of the Personal Data have:

3.1 committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in respect of the Personal Data; and

3.2 undertaken appropriate training in relation to protection of Personal Data.

3.3 Intellicene shall not operate or support the actual operation of its products and other solutions in Customer's real-life environment or in relation to Customer's objectives.

4. Security

4.1 Intellicene shall implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk in the provision of the Services and for the purposes of this DPA Intellicene's technical and organisational measures are set out at Annex 2 to this DPA.

4.2 In assessing the appropriate level of security, Intellicene shall take account in particular of the risks that are presented by Processing.

5. Subprocessing

5.1 Intellicene shall only appoint Subprocessors which enable Intellicene to comply with Privacy Laws. Customer authorises Intellicene to appoint Subprocessors in accordance with this Section 5 subject to any restrictions or conditions expressly set out in the Agreement.

5.2 Before Intellicene engages any new Subprocessor, Intellicene shall give Customer notice of such appointment. If, during that notice period, Customer notifies Intellicene of any objections (on reasonable grounds related to Privacy Laws) to the proposed Subprocessor ("**Objection**"), then Intellicene and Customer shall negotiate in good faith to agree to further measures including contractual or operational adjustments relevant to the appointment of the proposed Subprocessor or operation of the Services to address Customer's Objection. Where such further measures cannot be agreed between the parties within forty-five (45) days from Intellicene's receipt of the Objection (or such greater period agreed by Customer in writing) Customer may by written notice to Intellicene with immediate effect terminate that part of the Services which require the use of the proposed Subprocessor.

6. Data Subject Rights

6.1 Intellicene shall:

6.1.1 upon becoming aware, promptly notify Customer if Intellicene receives a request from a Data Subject relating to an actionable Data Subject right under any Privacy Law in respect of Personal Data;

6.1.2 upon request from Customer where required by Privacy Laws and in the context of the Services, reasonably assist Customer in dealing with an actionable Data Subject rights request to the extent Customer cannot fulfil this request without Intellicene's assistance. Intellicene may fulfil this request by making available functionality that enables Customer to address such Data Subject rights request without additional Processing by Intellicene. To the extent such functionality is not available, in order for Intellicene to provide such reasonable assistance, Customer must communicate such request in writing to Intellicene providing sufficient information to enable Intellicene to pinpoint and subsequently amend, export or delete the applicable record.

7. Personal Data Breach

7.1 Intellicene shall notify Customer without undue delay upon Intellicene or any Subprocessor becoming aware of a Personal Data Breach, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Privacy Laws. Such notification shall as a minimum:

7.1.1 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;

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

7.1.3 describe the likely consequences of the Personal Data Breach in so far as Intellicene is able to ascertain having regard to the nature of the Services and the Personal Data Breach; and

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

7.2 Intellicene shall co-operate with Customer and take such reasonable commercial steps as are necessary to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 Where and in so far as, it is not possible to provide the information referred to in Section 7.1 at the same time, the information may be provided in phases without undue further delay.

8. Data Protection Impact Assessment and Prior Consultation

8.1 To the extent necessary, Intellicene shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Privacy Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Intellicene. To the extent that such impact assessment and/or prior consultation requires assistance beyond Intellicene providing the applicable Intellicene processing record(s) and Documentation, Intellicene shall reserve the right to charge Customer such engagement at Intellicene's then current daily rates.

9. Deletion or return of Personal Data

9.1 Within thirty (30) days from termination or expiry of the Agreement (the "Return Period"), at Customer's request, Intellicene will either delete or return available Personal Data. At the expiry of the Return Period, if Customer has not elected either of the foregoing Intellicene may delete and destroy all Personal Data without notice or liability to Customer. Where Customer requests Intellicene return available Personal Data, Intellicene may fulfil this request by making available functionality that enables Customer to retrieve the Personal Data without additional Processing by Intellicene. If Customer declines to use this functionality, Customer may, within the Return Period, request that Intellicene return the available Personal Data under an Order for the applicable professional services. In the event the Agreement is terminated for Customer's breach, Intellicene shall have the right to require that Customer prepay for such professional services. Intellicene shall provide written confirmation to Customer that it has fully complied with this Section 9 within thirty (30) days of Customer's request for such confirmation.

9.2 Intellicene may retain Personal Data to the extent required by Privacy Laws or any other statutory requirement to which Intellicene is subject and only to the extent and for such period as required by Privacy Laws or any other statutory requirement to which Intellicene is subject and always provided the provisions of this DPA will continue to apply, that Intellicene shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Privacy Laws requiring its storage or any other statutory requirement to which Intellicene is subject and for no other purpose.

10. Review, Audit and Inspection rights

10.1 Upon Customer's reasonable request, Intellicene shall provide all relevant and necessary material, documentation and information in relation to Intellicene's technical and organisational security measures used to protect the Personal Data in relation to the Services provided in order to demonstrate compliance with Privacy Laws.

10.2 Intellicene shall ensure a security audit of its technical and organisational security measures is carried out at least annually in compliance with Privacy Laws and shall also:

10.2.1 be performed according to ISO 27001 standards;

10.2.2 be performed by qualified auditor ; and

10.2.3 result in the generation of a summary report.

Intellicene shall promptly provide Customer upon request with (i) a confidential summary of such report; and (ii) evidences of appropriate remediation of any critical issues within four (4) weeks from date of issuance of the audit report.

10.3 If, following the completion of the steps set out in Sections 10.1 and 10.2 Customer reasonably believes that Intellicene is non-compliant with Privacy Laws, Customer may request that Intellicene make available, either by webinar or in a face-to-face review, extracts of all relevant information necessary to further demonstrate compliance with Privacy Laws. Customer undertaking such review shall give Intellicene reasonable notice, by contacting privacypolicy@Intellicene.com, of any review to be conducted under this Section 10.3.

10.4 In the event that Customer reasonably believes that its findings following the steps set out in Section 10.3 do not enable Customer to comply materially with Customer's obligations mandated under the Privacy Laws in relation to its appointment of Intellicene, then Customer may give Intellicene not less than thirty (30) days prior written notice of its intention, undertake an audit which may include inspections of Intellicene to be conducted by Customer or an auditor mandated by Customer (not being a competitor of Intellicene). Such audit and/or inspection shall (i) be subject to confidentiality obligations agreed between Customer (or its mandated auditor) and Intellicene, (ii) be undertaken solely to the extent mandated by, and may not be further restricted under applicable Privacy Laws, (iii) not require Intellicene to compromise the confidentiality of security aspects of its systems and/or data processing facilities (including that of its Subprocessors), and (iv) not be undertaken where it would place Intellicene in breach of Intellicene's confidentiality obligations to other Intellicene customers vendors and/or partners generally or otherwise cause Intellicene to breach laws applicable to Intellicene. Customer (or auditor mandated by Customer) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to Intellicene's premises, equipment, personnel and business in the course of such a review. To the extent that such audit performed in accordance with this Section 10.4 exceeds one (1) business day, Intellicene shall reserve the right to charge Customer for each additional day at its then current daily rates.

10.5 If following such an audit or inspection under Section 10.4, Customer, acting reasonably, determines that Intellicene is non-compliant with Privacy Laws then Customer will provide details thereof to Intellicene upon receipt of which Intellicene shall provide its response and to the extent required, a draft remediation plan for the mutual agreement of the parties (such agreement not to be unreasonably withheld or delayed; the mutually agreed plan being the "Remediation Plan"). Where the parties are unable to reach agreement on the Remediation Plan or in the event of agreement, Intellicene materially fails to implement the Remediation Plan by the agreed dates which in either case is not cured within forty-five (45) days following Customer's notice or another period as mutually agreed between the Parties, Customer may terminate the Services in part or in whole which relates to the non-compliant Processing and the remaining Services shall otherwise continue unaffected by such termination.

10.6 The rights of Customer under Section 10 shall only be exercised once per calendar year unless Customer reasonably believes Intellicene to be in material breach of its obligations under either this DPA or Privacy Laws.

11. Restricted Transfers

11.1 Customer (as "data exporter") and Intellicene, as appropriate, (as "data importer") hereby agree that the Standard Contractual Clauses shall apply in respect of any Restricted Transfer from Customer to Intellicene. Each Party agrees to execute the Standard Contractual Clauses upon request of the other Party and further agree that absent of execution the terms and conditions of the Standard Contractual Clauses shall in any event apply to any Restricted Transfer. Where such Standard Contractual Clauses must be fully executed to take effect and Customer has not executed such Standard Contractual Clauses as set out in this Section 11, Customer authorises Intellicene to enter into the Standard Contractual Clauses for and on behalf of Customer as data exporter with each applicable data importer.

11.2 For the purposes of Appendix 1 or other relevant part of the Standard Contractual Clauses, Annex 1 to this DPA sets out the Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing (processing operations).

12. Other Privacy Laws

12.1 To the extent that Processing relates to Personal Data originating from a jurisdiction or in a jurisdiction which has any mandatory requirements in addition to those in this DPA, both Parties may agree to any additional measures required to ensure compliance with applicable Privacy Laws and any such additional measures agreed to by the Parties will be documented as an Annex to this DPA or in an Order to the Agreement. Due to the fact that Intellicene has no control over the type, character, properties, content, and/or origin of Personal Data Processed hereunder, notwithstanding anything to the contrary herein, Intellicene shall not be in breach of this DPA or the Agreement or liable to Customer to the extent Personal Data subject to jurisdictional requirements mandating security, processing or other measures not set forth in, or contrary to the terms of, this DPA is provided by Customer without amending this DPA or entering into an Order addressing the same.

12.2 If any variation is required to this DPA as a result of a change in Privacy Laws, including any variation which is required to the Standard Contractual Clauses, then either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to this DPA, including the Standard Contractual Clauses, to address such changes.

13. General Terms

13.1 The Intellicene contracting entity shall be the Intellicene entity set by the Agreement.

Order of precedence

13.2 In the event of inconsistencies between the provisions of this DPA and (i) Annex 2 (Information Security Schedule), or (ii) any other agreements between the parties, including the 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 DPA, the provisions of the Agreement shall prevail.

13.3 Even without signing this DPA itself, it will enter into force as of the signing of the Customer on the Agreement, with the reference to this DPA. Onless otherwise stated in this DPA, all other provisions of the Agreement shall apply and remain valid during the term of the Agreement and until its cessation, expiry or termination for any reason.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the last date of signature.

CUSTOMER (AS DEFINED ABOVE)

Signature _____

Name _____

Title _____

Date Signed _____, **20**_____

Intellicene

Signature:

Name as indicated on the above e-signature

Title as indicated on the above e-signature

Date Signed: as indicated on the above e-signature

Attached:

- Annex 1: Data Processing Instructions
- Annex 2: Information Security Schedule

ANNEX 1: DATA PROCESSING INSTRUCTIONS APPLICABLE TO NOWFORCE (SAAS) SOLUTION

Solution	**NowForce**
Processing Activity: **Support**	Product Support may be provided by Intellicene in accordance with Intellicene's Support Plan. Support may be provided either in the context of Software or Hosted Subscription Services. The Agreement and Order will set out the applicable Support Plan and that Support Plan sets out information on how Support is provided. When providing Support, Intellicene may be required by Customer to Process Personal Data. Intellicene may access and/or receive Personal Data when providing Support. Personal Data is not accessed and/or received in every service Support case because some errors can be analysed and rectified without such access if the background to the error is known. Depending on the issue, Intellicene Affiliates (listed below) may provide Support and therefore an international transfer of Personal Data may occur pursuant to Section 11 of the DPA.
Processing Activity: **Professional Services**	If, as part of an Order, Customer requires Intellicene to perform professional services to assist in deployment of the product or Managed Services during the term, then Intellicene may be required by Customer to Process Personal Data as part of this engagement.
Processing Activity: **Hosted Subscription Services**	Customer will upload data to the Hosted Subscription Services in order to maximise the functionality of the product. Some of the data which may be uploaded to the Hosted Subscription Services includes Personal Data. Intellicene will host (storage) the data on behalf of Customer in accordance with the terms and conditions of service under the Agreement as mutually agreed to by the Parties. Intellicene may use a Subprocessor to deliver cloud hosting services as outlined below. Customer will determine how and why the product will be used to its benefit which may include the frequent or infrequent use of Personal Data. Customer acknowledges that in relation to these Processing operations, Intellicene has no control over the submission of Data Subject's Personal Data and that the design of the data to be submitted to Intellicene's hosted services is at all times under the control of Customer. Except for the underlying cloud storage of the SaaS services (and the provision of Support, if applicable, described above), Intellicene is not involved in any Processing activities associated with this use of the product. If, as part of an Order, Customer requires Intellicene to perform professional services to assist in deployment of the product or Managed Services during the Term, then Intellicene may be required by Customer to Process Personal Data for those purposes.
Categories of Personal Data	▪ Customer's employee categories: name, title, contact details, department, ID number, , , email address. ▪ Customer's end-user categories: name, email address, contact telephone number, contact history,. Additional Categories of Personal Data may be provided by Customer either as part of a Support request or through Customer's use of Hosted Subscription Services.
Special Categories of Personal Data	As Additional Categories of Personal Data may be provided by Customer either as part of a Support request or through Customer's use of Hosted Subscription Services it is possible that from time-to-time Customer instructs Intellicene to Process Special Categories of Data. Intellicene's products do not typically process Special Categories of Personal Data however Customer may determine that such categories will be Processed. Where applicable, Customer must inform Intellicene of this intention prior to conducting the Processing.
Data Subjects	Employees, clients, customers and suppliers of Customer. Employees or contractors of Customer who contact Intellicene's technical support facilities. Customer determines which Data Subjects form part of the Processing and therefore these categories may change depending on Customer's use of the product.
Duration of Processing	Support & Professional Services: Personal Data is processed only for as long as is necessary to provide the particular Support and/or Professional Services. SaaS: Personal Data is stored for the duration of the Services and is deleted or returned to Customer as set out under Section 9 of the DPA or as otherwise amended or deleted by Customer during the Term.
Intellicene Affiliate(s) as Subprocessors	The following non-exhaustive list of Intellicene Affiliates may be considered Subprocessors in circumstances set out in this table and may provide technical support services, project related services, back office systems, data transfer and storage, and backup and disaster recovery services: EMEA: Intellicene Software UK Limited, UK; Symphia Intellicene Software Ltd., Israel. Americas: Intellicene Software Ltda., Brazil; Enterprise Intellicene Canada Inc.,Canada APAC: Intellicene India Private Limited, India.

We use Amazon availability zone service https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/\using-regions-availability-zones.html#concepts-availability-zones

ANNEX 2: INFORMATION SECURITY SCHEDULE

1 DEFINITIONS. In addition to the capitalized terms in the Agreement and the DPA, all capitalized terms shall have the meaning ascribed to them herein this Annex, and for the purposes of this Annex, shall govern and control in the event of any conflict, including the following:

1.3 Customer Data. All data provided by Customer to Intellicene where such data contains Personal Data, or with respect to Hosted Subscription Services, data collected or generated by Hosted Subscription Services on Customer's behalf, and remains in Intellicene's possession and control for further Processing.

1.4 Encryption Standards. Encryption algorithms that are publicly or commercially available, with key lengths sufficient to prevent commercially reasonable attempts to decrypt through brute force the encrypted information.

1.5 Hosted Subscription Services. Any SaaS or hosting services subscribed to by Customer from Intellicene.

1.6 Industry Standards. Generally accepted standards applicable to the performance obligations of a party with respect to a product or service. Industry Standards can include in part or in whole frameworks published by the National Institutes for Standards and Technology (NIST), International Organization for Standardization, ISACA, Payment Card Industry Security Standards Council and other internationally recognized standards organizations.

1.7 Intellicene Personnel. Each Intellicene employee or subcontractor under obligations of confidentiality and nondisclosure which performs on behalf of Intellicene hereunder.

2 GENERAL SECURITY TERMS. Intellicene is committed to helping protect the security of Customer Data, and has implemented, and will maintain and follow appropriate technical and organizational measures that conform to Industry Standards intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. Intellicene may modify any of its policies, process or procedures at any time and without obligation to notify or update this Annex, provided such modifications provide substantially similar or greater protections than those provided for herein.

3 SAAS AND HOSTING SECURITY TERMS. the following terms and conditions shall apply to Intellicene's performance obligations with respect to any Hosted Subscription Services procured by Customer under this Agreement.

3.1 Access Controls. Customer shall have access to Customer Data maintained within their applicable production instance. Customer shall be responsible for maintaining user access and security controls for users accessing the Hosted Subscription Services. Intellicene shall be responsible for restricting all other access to Customer Data residing within the production instance. For the avoidance of doubt, Intellicene has no obligation to verify that any user using Customer's account and password has Customer's authorization. Intellicene shall provide access on a need to know basis and shall review access rights of Intellicene Personnel at least annually. Intellicene's access controls shall include no less than the following:

- Intellicene shall enforce complex passwords using built in system settings of at least 8 characters. Intellicene shall require password changes at least every ninety (90) days. Intellicene administrators shall use multi-factor authentication for access to the production environment(s).
- Access to Intellicene's production environment(s) is controlled at four distinct hierarchical levels: the hosting partner level, the SaaS operations team level, the Intellicene network security level, and the application level. Access control is required for each of these levels to provide the optimal level of security for the solution.
- An Intellicene hosting partner's role is to design, deploy, secure, make available, and support the systems upon which Intellicene's SaaS solutions are installed and delivered to Intellicene's customers (end users). The hosting partners have primary control over the data centers, systems, and networks upon which Intellicene's SaaS solutions operate. The hosting partner provides Intellicene's SaaS operations team with the initial credentials required to access the hosted systems and support portals.

3.2 Data Controls. In its performance obligations with respect to Hosted Subscription Services, Intellicene does require access to Customer Data, and the following additional terms and conditions shall apply:

- Intellicene's security procedures shall require that any Customer Data stored by Intellicene only be stored using secure data encryption algorithms and key strengths of 128-bit symmetric and 1024-bit asymmetric or greater. Intellicene shall monitor Industry Standards and implement an action plan if key lengths in use can be compromised through commercially reasonable means.
- Intellicene will maintain a key management process that includes appropriate controls to limit access to private keys and a key revocation process. Private keys, and passwords shall not be stored on the same media as the data they protect.
- Intellicene will prohibit Intellicene Personnel from the download, extraction, storage or transmission of Customer Data through personally owned computers, laptops, tablet computers, cell phones, or similar personal electronic devices except where enrolled in Intellicene's Mobile Device Management (MDM), Information Rights Management (IRM), or other security programs. If personal computers or mobile devices are used to perform any part of the Hosted Subscription Services, Intellicene will encrypt all Customer Data on such mobile devices.
- Intellicene agrees that any and all electronic transmission or exchange of Customer Data shall be protected by a secure and encrypted means (e.g. HTTPS, SSH, encryption using TLS on gateway while sending emails).
- Customer Data stored as a part of the Hosted Subscription Services shall reside only on Intellicene production systems housed in Intellicene hosting partner data centers, unless noted in a SOW or required with respect to professional service engagements or performance of support services. Any storage of Customer Data on Intellicene premises is temporary and is used strictly for support and services engagements. Once Customer Data on Intellicene premise has served its purpose, it shall be promptly destroyed in accordance to Intellicene's confidential data destruction procedures.
- Intellicene will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. Intellicene will ensure that transfers of Personal Data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR and that such transfers and safeguards are documented according to Article 30(2) of the GDPR.

3.3 Operational Controls. In its performance of Hosted Subscription Services, Intellicene shall maintain operational controls sufficient to enable Intellicene's satisfaction of its performance obligations in this Section 3, including, without limitation, the following:

- Intellicene will utilize up-to-date and comprehensive virus and malware protection capabilities, and commercially reasonable practices, including detection, scanning and removal of known viruses, worms and other malware on the Intellicene's hosting systems. These virus protection capabilities will be in force on all computers and/or devices utilized in connection with the technology services, as well as on all data files or other transfers that have access or are connected to Intellicene's hosting system.
- If a virus, worm or other malware causes a loss of operational efficiency or loss of data, Intellicene will mitigate losses and restore data from the last virus free backup to the extent practicable.
- Intellicene shall obligate its hosting partners to provide a multiple layered security approach. This shall include perimeter firewalls, DMZ, one or more internal network segments, and network intrusion detection monitors for attempted intrusion to the production environment. Network vulnerability scans shall be conducted regularly and issues addressed according to Industry Standard change control processes.
- Intellicene shall mitigate security vulnerabilities through the use of perimeter and host countermeasures such as intrusion prevention, web application firewall, IP address shunning, and other measures designed to prevent successful exploitation of vulnerabilities.
- Intellicene and its hosting partners shall proactively address security risks by applying released security patches, including, as example, Windows security patching and updates to patch known vulnerabilities in an applicable operating system. Patches shall be deployed to production via Intellicene's change management process. Intellicene shall test all patches in its test environment prior to release to production. If a patch degrades or disables the production environment, Intellicene shall continue to mitigate vulnerabilities until a patch is provided by the software or operating system manufacturer that does not degrade or disable production. Such mitigation efforts may include intrusion prevention, web application firewall, and other measures chosen by Intellicene to reduce likelihood or prevent successful access to Customer Data by an unauthorized party.
- Each month, Intellicene and its hosting partners shall schedule maintenance windows to perform data center, system, and application maintenance activities. Intellicene shall notify Customer in advance of any scheduled maintenance activity that is expected to disrupt the Hosted Subscription Services functionality.

- Intellicene shall retain security logs for a minimum of thirty (30) days online and ninety (90) days archived. Intellicene may retain logs for a longer period at its sole discretion.

3.4 **Availability Controls.** With respect to Hosted Subscription Services:

- Intellicene shall maintain business continuity and disaster recovery plans specific to its Hosted Subscription Services, and shall include data center failover configurations.
- Intellicene shall maintain a backup of all Customer Data that Intellicene is required to retain as a part of the Hosted Subscription Services. In the event Customer Data becomes destroyed or corrupt, Intellicene shall use commercially reasonable efforts to restore all available data from backup, and remediate and recover such corrupt data.

3.5 **Application Controls.** Intellicene shall implement and conform its software development practices to applicable Industry Standards relative to the functionality to be performed by the specific Intellicene product offering. Intellicene shall maintain software development practices which satisfy the following:

- Use commercially reasonable measures to detect product vulnerabilities prior to release. These measures may include manual test scripts, test automation, dynamic code analysis, static code analysis, penetration testing, or other measures chosen by Intellicene. Intellicene shall update procedures and processes from time to time to improve detection of vulnerabilities within its products.
- Intellicene's developers shall not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any systems or network.
- Intellicene's developers shall receive regular training on coding and design with respect to application security.

4 **ATTESTATIONS OF COMPLIANCE.** Intellicene shall provide attestation of compliance to the terms in this Annex. Requests shall be made in writing through the Account Executive assigned to Customer. Intellicene shall provide its Santa Fe Group Standard Information Gathering Questionnaire applicable to the services provided to Customer. Intellicene shall respond to such attestation requests within thirty (30) business days of receipt.