GENERAL TERMS AND CONDITIONS FOR RESALE OF CLOUD SERVICES

Last Updated: 20260525
Version: 20260525v1

These General Terms and Conditions for Resale of Cloud Services ("GTC") govern operational and technical aspects of the Cloud Services provided by Innology Ventures, S.L. ("Company") to end customers ("Customers") through authorized resale partners ("Partners"). These GTC may be updated from time to time as set forth herein.

1. END USER LICENSE AGREEMENT (EULA)

1.1 **Scope**. This EULA governs the relationship between Company and each end customer ("Customer") that accesses or uses the Cloud Services through an authorized Partner.

1.2 **Grant of License**. Subject to the terms of this EULA, Company grants Customer a non-exclusive, non-transferable, non-sublicensable, revocable right to access and use the Cloud Services solely for Customer's internal business purposes during the Subscription Term specified in the applicable Order Form, and solely in accordance with the Usage Metrics specified therein, and solely within the territory defined in the applicable terms governing the provision of the Cloud Services, or, in the absence of such definition, within the territory where Customer is domiciled. This license may be revoked by Company upon Customer's material breach of any obligation under this EULA, the GTC, or any other applicable terms governing the use of the Cloud Services.

1.3 **Usage Restrictions**. Customer shall not, and shall not permit any third party to: (a) use the Cloud Services for any purpose other than Customer's internal business operations; (b) sublicense, resell, rent, lease, or otherwise provide access to the Cloud Services to any third party; (c) use the Cloud Services to provide services to third parties (service bureau or time-sharing arrangements); (d) exceed the authorized Usage Metrics; (e) access the Cloud Services through any unauthorized means; (f) use the Cloud Services in violation of the Acceptable Use Policy; or (g) grant access to the Cloud Services to any competing company, understanding as such any entity that develops, markets, or distributes products or services similar or analogous to the Cloud Services.

1.4 **User Accounts and Credentials**. Customer is responsible for: (a) maintaining the confidentiality and security of all user accounts and access credentials; (b) all activities that occur under Customer's accounts; (c) ensuring that users do not share credentials; and (d) promptly notifying Company of any unauthorized access or security breach. User credentials may be reassigned to different individuals when the original user no longer requires access, but credentials may not be shared among multiple simultaneous users. Access to the Cloud Services is permitted to Customer's employees and to any individual to whom Customer has granted access credentials, regardless of whether such individual acts on Customer's behalf at the time of access. Customer remains fully liable for any breach of this EULA or the GTC caused by any individual to whom Customer has granted or failed to revoke access.

1.5 **Customer Data Ownership**. As between Company and Customer, Customer retains all ownership rights in Customer Data. Customer grants Company a limited license to process Customer Data solely as necessary to provide the Cloud Services and as set forth in the Data Processing Agreement.

1.6 **Company's Rights to Suspend**. Company may suspend Customer's access to the Cloud Services if: (a) Customer breaches this EULA or the Acceptable Use Policy; (b) Customer's use poses a security risk to the Cloud Services or other customers; (c) Customer's account is more than fifteen (15) days overdue on payment to Partner, upon notification from Partner or upon Company becoming aware of such overdue payment by any other means; or (d) required by law or court order. Company shall provide prompt notice of suspension to both Partner and Customer (except where prohibited by law) and shall limit suspension to the minimum scope and duration reasonably necessary.

1.7 **Term and Termination**. This EULA remains in effect for the Subscription Term. Upon expiration or termination: (a) Customer's right to access the Cloud Services immediately terminates; (b) Customer is responsible for exporting all Customer Data prior to the expiration or termination of the Subscription Term; (c) upon Customer's express written request submitted before the expiration or termination date, and provided that Customer is in full compliance with all obligations under this EULA and the GTC, Company may, at its sole discretion, grant Customer an additional period of up to thirty (30) days solely for the purpose of exporting Customer Data, after which Company may delete all Customer Data unless required to maintain it or unless Company is entitled to retain it under applicable law, including the retention of a duly blocked copy of Customer Data for compliance purposes or the exercise and defense of legal claims; (d) Customer must immediately cease all use of the Cloud Services and Documentation except during any additional export period granted pursuant to (c) above; and (e) all provisions that by their nature should survive (including payment obligations, intellectual property rights, limitation of liability, and confidentiality) shall survive.

1.8 **Warranties**. COMPANY WARRANTS THAT THE CLOUD SERVICES WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH THE DOCUMENTATION. EXCEPT AS EXPRESSLY SET FORTH IN THIS PROVISION, THE CLOUD SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. COMPANY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, QUIET ENJOYMENT, AND ACCURACY. COMPANY DOES NOT WARRANT THAT THE CLOUD SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE, OR THAT ALL DEFECTS WILL BE CORRECTED.

1.9 **Limitation of Liability**. NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THIS EULA OR THE CLOUD SERVICES, REGARDLESS OF THE CAUSE OF ACTION OR THE THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. COMPANY'S TOTAL LIABILITY TO CUSTOMER SHALL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER (THROUGH PARTNER) FOR THE CLOUD SERVICES DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO LIABILITY. THE FOREGOING LIMITATIONS SHALL NOT APPLY TO: (a) CUSTOMER'S PAYMENT OBLIGATIONS; (b) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (c) FRAUD OR FRAUDULENT MISREPRESENTATION; (d) BREACHES OF CONFIDENTIALITY; OR (e) LIABILITIES THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

1.10 **Third-Party Beneficiary**. Partner is a third-party beneficiary of this EULA solely for the purpose of enforcing Customer's compliance with payment obligations owed to Partner.

2. ACCEPTABLE USE POLICY

2.1 **Prohibited Uses**. Customers and Partners shall not, and shall not permit any user to, use the Cloud Services to:

(a) Illegal Activities: Engage in any illegal activity, violate any applicable law or regulation, or violate the rights of others;

(b) Harmful Content: Upload, transmit, store, or process any content that: (i) is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, or otherwise objectionable; (ii) infringes any patent, trademark, trade secret, copyright, or other intellectual property or proprietary rights; (iii) violates any person's rights of privacy or publicity; (iv) contains software viruses, malware, ransomware, or any other malicious code; or (v) contains false, misleading, or fraudulent information;

(c) Security Violations: (i) Attempt to gain unauthorized access to the Cloud Services or related systems or networks; (ii) use any automated means (including robots, spiders, or scrapers) to access the Cloud Services except as expressly permitted; (iii) probe, scan, or test the vulnerability of the Cloud Services or any related system or network; (iv) breach or circumvent

any security or authentication measures; (v) interfere with service to any user, host, or network (including denial of service attacks, flooding, or mail bombing); or (vi) forge any TCP/IP packet header or any part of the header information;

(d) Network Abuse: (i) Send unsolicited or unauthorized advertising, spam, chain letters, or other forms of commercial solicitation; (ii) use the Cloud Services to transmit material that contains excessive volume or bandwidth usage; or (iii) use the Cloud Services in a manner that adversely impacts the performance or availability of the Cloud Services for other users;

(e) Reverse Engineering: Reverse engineer, decompile, disassemble, or attempt to derive the source code, algorithms, or structure of the Cloud Services;

(f) Competitive Uses: Use the Cloud Services to develop, market, or support any product or service that competes with Company's offerings, or conduct competitive benchmarking or analysis without Company's prior written consent; or grant access to the Cloud Services to any competing company, understanding as such any entity that develops, markets, or distributes products or services similar or analogous to the Cloud Services;

(g) Circumvention: Remove, alter, or obscure any proprietary notices on the Cloud Services, or attempt to circumvent Usage Metrics or usage limitations.

2.2 **Usage Monitoring**. Company reserves the right to monitor usage of the Cloud Services to ensure compliance with this Acceptable Use Policy and to protect the security and integrity of the Cloud Services. Company may investigate suspected violations and cooperate with law enforcement authorities.

2.3 **Enforcement**. If Company determines that Customer or any user has violated this Acceptable Use Policy, Company may: (a) suspend or terminate access to the Cloud Services; (b) remove or disable access to violating content; (c) report violations to law enforcement; or (d) take any other action Company deems appropriate. Company shall provide notice to Partner and Customer (except where prohibited by law) and an opportunity to remedy non-material violations before suspending or terminating access.

2.4 **Reporting Violations**. If Customer or Partner becomes aware of any violation of this Acceptable Use Policy, they shall promptly notify Company at ciso-office@opinator.com.

3. SERVICE LEVEL AGREEMENT (SLA)

3.1 **Uptime Commitment**. Company will ensure that the Cloud Services have an availability level of 99%, excluding when the Cloud Services are unavailable due to: (a) required system maintenance as determined by Company; and (b) causes outside of the reasonable control of Company that could not have been avoided by its exercise of due care ("Availability"). "Downtime" means time during which the Cloud Services have no Availability.

3.2 **Specific SLA.** The parties may agree on additional or different service level commitments applicable to specific Cloud Services or Customer requirements. Any such specific service level agreement shall be documented in a separate annex or the applicable Order Form and shall prevail over the standards set forth in this Section 3 to the extent of any conflict.

4. SECURITY AND COMPLIANCE STANDARDS

4.1 **Security Measures**. Company implements and maintains technical and organizational security measures to protect the Cloud Services and Customer Data, including:

(a) Access Controls: Role-based access controls, multi-factor authentication for administrative access, and principle of least privilege;

(b) Encryption: Encryption of data in transit using TLS 1.2 or higher, and encryption of data at rest using AES-256 or equivalent;

(c) Network Security: Firewalls, intrusion detection/prevention systems, network segmentation, and DDoS protection;

(d) Vulnerability Management: Regular security assessments, penetration testing (at least annually), vulnerability scanning, and prompt patching of security vulnerabilities;

(e) Security Monitoring: 24/7 security monitoring, logging of security events, and incident detection and response procedures;

(f) Physical Security: Data centers with controlled physical access, environmental controls, redundant power and cooling, and fire suppression systems;

(g) Backup and Recovery: Regular backups of Customer Data (daily full) with retention for thirty (30) days, and tested disaster recovery procedures;

(h) Secure Development: Secure software development lifecycle, code reviews, security testing, and change management procedures.

4.2 **Security Certifications and Audits**. Company maintains the following security certifications and undergoes regular audits:

(a) ISO/IEC 27001: Information Security Management System certification;

(b) GDPR Compliance: Compliance with EU General Data Protection Regulation requirements;

(c) Additional certifications may be obtained and will be listed on Company's website.

4.3 **Security Incident Response**. In the event of a security incident affecting Customer Data:

(a) Company shall notify Partner and Customer without undue delay and in any event within seventy-two (72) hours of becoming aware of the incident (or sooner if required by applicable law or by specific terms and conditions expressly agreed in writing between Customer and Company);

(b) The notification shall include: (i) description of the nature of the incident; (ii) categories and approximate number of affected customers and data records; (iii) likely consequences; (iv) measures taken or proposed to address the incident; and (v) contact point for further information;

(c) Company shall investigate the incident, take steps to mitigate harm, and implement measures to prevent recurrence;

(d) Company shall cooperate with Customer in fulfilling any legal obligations to notify data protection authorities or data subjects;

(e) Company shall provide periodic updates on the investigation and remediation.

4.4 **Penetration Testing by Customers**. Customers may request to conduct penetration testing of their use of the Cloud Services subject to the following:

(a) Customer must provide at least thirty (30) days' advance written notice to Company and obtain Company's prior written consent before conducting any penetration testing. Company's consent may be withheld or conditioned at Company's sole discretion;

(b) Prior to commencing any penetration testing, Customer and the appointed third-party security firm must execute a non-disclosure agreement in a form acceptable to Company, covering all information obtained during or as a result of the testing;

(c) Testing must be conducted by a reputable third-party security firm approved in advance by Company;

(d) Testing must be limited in scope to Customer's own environment and data and exclusively to the resources, systems, and infrastructure directly associated with the Cloud Services provided to Customer under the applicable Order Form. Any extension of scope requires separate written consent from Company;

(e) Testing must not disrupt the Cloud Services or affect other customers or Company's infrastructure. Customer shall immediately suspend testing upon Company's request if Company determines, at its sole discretion, that the testing poses a risk to the Cloud Services or other customers;

(f) Customer must provide Company with a copy of the test results within fifteen (15) days of completion of the testing. Such results shall be treated as Confidential Information of both parties;

(g) Testing must be conducted during agreed time windows as specified in Company's written consent, and must not exceed the duration, frequency, or technical parameters set forth therein;

(h) Customer shall be responsible for any damages, disruptions, or security incidents arising out of or in connection with the penetration testing. Customer shall ensure that the appointed third-party security firm assumes joint responsibility for any such damages, disruptions, or security incidents caused by its actions or omissions during the testing.

(i) Company reserves the right to deny, limit, suspend or revoke testing consent that could impact service availability or security, without incurring any liability towards Customer.

4.5 **Security Updates**. Company shall use commercially reasonable efforts to provide security updates and patches for the Cloud Services, to the extent within Company's reasonable control, as follows: (a) Critical security vulnerabilities shall be patched within fifteen (15) days, where technically feasible; (b) High-severity vulnerabilities shall be patched within thirty (30) days, where technically feasible; (c) Company shall notify Partners and Customers of security updates that may impact functionality or require Customer action; (d) Customers are responsible for updating integrations or client-side components as specified in update notifications.

4.6 **Subprocessors**. Company may use third-party subprocessors to assist in providing the Cloud Services. A current list of subprocessors is available at https://web.opinator.com/legal/subprocessors and is updated as subprocessors are added or changed. Company shall: (a) enter into written agreements with subprocessors that include data protection obligations at least as protective as those in the Data Processing Agreement; (b) remain responsible for subprocessor compliance; and (c) provide at least thirty (30) days' notice before adding or replacing subprocessors, during which time Customer may object if the change creates material risks.

5. PARTNER CODE OF CONDUCT

5.1 **Ethical Business Practices**. Partners shall conduct business with integrity and in compliance with all applicable laws. Partners shall:

(a) Anti-Corruption: Not engage in bribery, corruption, or any form of improper payment or inducement. Partners shall comply with all applicable anti-corruption laws, including the US Foreign Corrupt Practices Act (FCPA), UK Bribery Act 2010, and local anti-corruption laws;

(b) Gifts and Entertainment: Not offer or accept gifts, meals, entertainment, or other business courtesies that could create an improper influence or appearance of impropriety. Modest gifts and business meals are permitted if they: (i) are infrequent and reasonable in value (generally under 250 EUR); (ii) are not given in cash or cash equivalents; (iii) are transparent and properly documented; and (iv) do not violate local laws or the recipient's policies;

(c) Conflicts of Interest: Disclose any actual or potential conflicts of interest to Company and take appropriate steps to avoid or mitigate such conflicts;

(d) Government Officials: Exercise special caution when dealing with government officials, employees of state-owned entities, or political parties. Any gifts, hospitality, or payments to such individuals must be pre-approved by Company and comply with applicable laws;

(e) Accurate Records: Maintain accurate books and records that properly reflect all business transactions and comply with applicable accounting standards and tax laws;

(f) No Facilitation Payments: Not make facilitation payments (small payments to government officials to expedite routine actions), even if such payments are permissible under local law.

5.2 **Fair Competition**. Partners shall:

(a) Comply with all applicable antitrust and competition laws;

(b) Not engage in price fixing, market allocation, bid rigging, or other anti-competitive practices;

(c) Not disparage Company's competitors or make false or misleading statements about competing products;

(d) Not obtain competitors' confidential information through improper means;

(e) Compete fairly on the merits of Company's Cloud Services.

5.3 **Accurate Marketing and Sales Practices**. Partners shall:

(a) Accurately represent Company's Cloud Services in accordance with Company-provided materials;

(b) Not make false, misleading, or unauthorized claims about the Cloud Services, their capabilities, performance, security, or compliance;

(c) Not promise features, functionality, or service levels not documented in these GTC;

(d) Clearly distinguish between Company's Cloud Services and Partner's own services;

(e) Comply with all applicable advertising and consumer protection laws;

(f) Not engage in deceptive trade practices or unfair methods of competition.

5.4 **Data Protection and Privacy**. Partners shall:

(a) Comply with all applicable data protection and privacy laws, including GDPR;

(b) Only process personal data for legitimate business purposes and in accordance with applicable law;

(c) Implement appropriate technical and organizational measures to protect personal data;

(d) Provide clear privacy notices to customers and obtain necessary consents;

(e) Respond promptly to data subject rights requests;

(f) Report any personal data breaches to Company and affected individuals as required by law;

(g) Not sell, rent, or otherwise disclose customer personal data to third parties without consent;

(h) Ensure any third parties engaged by Partner comply with data protection obligations.

5.5 **Respect for Human Rights**. Partners shall:

(a) Respect fundamental human rights and dignity;

(b) Not use forced, bonded, or child labor;

(c) Provide fair wages, working hours, and conditions;

(d) Treat employees with respect and dignity;

(e) Not discriminate on the basis of race, color, religion, gender, age, disability, sexual orientation, or other protected characteristics;

(f) Provide a safe and healthy work environment;

(g) Respect employees' rights to freedom of association and collective bargaining.

5.6 **Environmental Responsibility**. Partners are encouraged to:

(a) Minimize environmental impact of their operations;

(b) Comply with all applicable environmental laws and regulations;

(c) Properly manage and dispose of waste;

(d) Seek to reduce energy consumption and greenhouse gas emissions;

(e) Promote sustainable business practices.

5.7 **Trade Compliance**. Partners shall:

(a) Comply with all applicable export control, sanctions, and trade restriction laws;

(b) Not provide Cloud Services to prohibited parties or in prohibited jurisdictions;

(c) Conduct appropriate screening of customers and transactions;

(d) Obtain necessary export licenses or authorizations;

(e) Not re-export or transfer the Cloud Services in violation of applicable laws;

(f) Maintain records demonstrating compliance with trade laws.

5.8 **Reporting Violations**. Partners shall:

(a) Promptly report to Company any suspected violations of this Code of Conduct or applicable laws;

(b) Cooperate with Company and government authorities in any investigations;

(c) Not retaliate against anyone who reports suspected violations in good faith;

(d) Maintain a compliance program appropriate to the size and nature of their business.

Reports can be made to: ciso-office@opinator.com.

5.9 **Consequences of Violations**. Violations of this Code of Conduct may result in:

(a) Suspension of Partner's right to submit new orders;

(b) Termination of the partnership arrangement;

(c) Legal action to recover damages;

(d) Reporting to law enforcement or regulatory authorities;

(e) Other remedies available under applicable agreements or law.

6. DATA PROCESSING AGREEMENT (DPA)

6.1 **Roles and Scope**. For the purposes of the GDPR and other applicable data protection laws:

(a) Customer is the data controller (or equivalent role) of any personal data contained in Customer Data;

(b) Company is the data processor (or equivalent role) acting on behalf of Customer;

(c) This DPA applies to Company's processing of personal data contained in Customer Data in connection with providing the Cloud Services;

(d) Partner is not a data processor merely by virtue of reselling the Cloud Services, unless Partner also processes Customer Data on behalf of Customer.

6.2 **Processing Instructions**. Company shall process personal data only: (a) as necessary to provide the Cloud Services; (b) as documented in Customer's configuration and use of the Cloud Services; (c) as instructed by Customer through the Cloud Services; and (d) as required by applicable law. If Company is required by law to process personal data in a manner not instructed by Customer, Company shall notify Customer of such requirement before processing (unless prohibited by law).

6.3 **Data Subject Rights**. Company shall, to the extent legally permitted and technically feasible, assist Customer in fulfilling Customer's obligations to respond to requests from data subjects exercising their rights under applicable data protection laws, including rights to access, rectification, erasure, restriction of processing, data portability, objection, and not to be subject to automated decision-making, including profiling. Company shall: (a) provide Customer with the ability to retrieve, correct, and delete Customer Data through the Cloud Services; (b) notify Customer promptly and, as a general rule, within five (5) business days of receipt, unless a shorter period is required by applicable law, if Company receives a request from a data subject; and (c) forward any data subject request received to Customer without delay, it being understood that the obligation to respond to such requests corresponds exclusively to Customer as data controller. Company shall not assume any responsibility for responding to data subject requests unless expressly agreed in writing as part of the scope of the Cloud Services in the applicable contractual documents. The time and resources devoted by Company to activities related to data subject requests shall, to the extent not already covered by the contracted scope of the Cloud Services, be considered part of the contracted service hours or billed to Customer as additional services at Company's then-current rates.

6.4 **Security Measures**. Company shall implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure. These measures are described in the Security and Compliance Standards section and shall be reviewed and updated regularly to ensure they remain appropriate.

6.5 **Subprocessors**. Company may engage subprocessors to assist in processing personal data, subject to the provisions on subprocessors in the Security and Compliance Standards section. Customer authorizes Company to engage the subprocessors listed at https://web.opinator.com/legal/subprocessors. Company shall: (a) enter into written agreements with subprocessors that include data protection obligations at least as protective as those in this DPA; (b) remain liable for subprocessor compliance; and (c) provide at least thirty (30) days' notice before adding or replacing subprocessors. If Customer objects to a new subprocessor on reasonable data protection grounds, the parties shall work in good faith to resolve the concern. If resolution is not possible, Customer may terminate the affected services.

6.6 **International Data Transfers**. Company may transfer personal data to countries outside the European Economic Area (EEA), UK, or Switzerland. For transfers subject to GDPR Chapter V, Company shall ensure that appropriate safeguards are in place, including:

(a) Standard Contractual Clauses (SCCs): The parties shall execute the applicable module of the EU SCCs as adopted by the European Commission, selecting the module that corresponds to the roles of the parties in each case (Module One: Controller to Controller; Module Two: Controller to Processor; or Module Three: Processor to Processor, as applicable). The applicable SCCs shall be executed as a separate document and are incorporated into this DPA by reference upon execution;

(b) UK and Swiss Transfers: For transfers subject to UK or Swiss law, the parties shall execute the applicable UK International Data Transfer Addendum or Swiss Federal Data Protection Act amendments to the Standard Contractual Clauses;

(c) Additional Safeguards: Company implements supplemental security measures for international transfers, including encryption, access controls, and data minimization;

(d) Transfer Impact Assessment: Company has conducted a transfer impact assessment and determined that, together with the Standard Contractual Clauses and supplemental security measures, transfers provide an adequate level of protection. Company shall notify Customer if it becomes aware of any circumstances that may affect this determination.

6.7 **Data Breach Notification**. Company shall notify Customer without undue delay after becoming aware of any personal data breach affecting Customer Data, and in any event within seventy-two (72) hours (or sooner if required by applicable law or by specific terms and conditions expressly agreed in writing between Customer and Company). The notification shall include the information specified in the Security Incident Response provisions and shall enable Customer to fulfill any breach notification obligations under applicable data protection laws.

6.8 **Audits and Compliance**. Upon Customer's reasonable request and with at least thirty (30) days' advance notice, Company shall: (a) make available to Customer information necessary to demonstrate compliance with this DPA; (b) allow for and contribute to audits or inspections conducted by Customer or an independent auditor appointed by Customer; provided that: (i) audits shall not occur more than once per year unless required by data protection authorities or following a personal data breach; (ii) the auditor shall execute a confidentiality agreement acceptable to Company; (iii) audits shall be conducted during business hours in a manner that minimizes disruption; and (iv) Customer shall bear the costs of audits except where audits reveal material non-compliance.

6.9 **Return and Deletion of Data**. Upon termination or expiration of the Cloud Services: (a) Customer is responsible for exporting all Customer Data prior to the expiration or termination of the Subscription Term; (b) upon Customer's express written request submitted before the expiration or termination date, and provided that Customer is in full compliance with all obligations under this EULA and the GTC, Company may, at its sole discretion, grant Customer an additional period of up to thirty (30) days solely for the purpose of exporting Customer Data; (c) following the expiration of any applicable retrieval period, Company shall delete all Customer Data (including copies), unless Company is entitled to retain it under applicable law, including the retention of a duly blocked copy for compliance purposes or the exercise and defense of legal claims, in which case such retained data shall remain subject to confidentiality obligations and shall be deleted when the legal retention requirement ends; (d) upon Customer's request prior to deletion,

Company shall make Customer Data available for export in a standard machine-readable format; and (e) Company shall provide written certification of deletion upon Customer's written request.

6.10 **Data Protection Impact Assessments**. If Customer is required to conduct a data protection impact assessment (DPIA) under GDPR Article 35, Company shall provide reasonable assistance and information necessary for the DPIA, taking into account the nature of processing and information available to Company.

6.11 **Contact for Data Protection Matters**. Customer may contact Company's CISO Office, responsible for Information Security, data protection, and compliance matters, regarding any questions or concerns about data protection at: ciso-office@opinator.com.

7. TECHNICAL DOCUMENTATION

7.1 **Documentation Availability**. Company provides comprehensive technical documentation for the Cloud Services, which may be requested by Customer provided that there is a valid agreement for the provision of Cloud Services in force and the requested documentation is relevant to the Cloud Services contracted by Customer. Such documentation may include:

(a) User Guides: End-user documentation for using the Cloud Services;

(b) Administrator Guides: Documentation for administrators managing the Cloud Services;

(c) Release Notes: Descriptions of new features, enhancements, bug fixes, and known issues for each release.

7.2 **Documentation License**. Company grants Partners and Customers a non-exclusive, non-transferable, non-sublicensable, revocable license to access and use the Documentation solely for Customer's internal business purposes in connection with their use of the Cloud Services during the Subscription Term. This license may be revoked by Company upon Customer's or Partner's material breach of any obligation under this EULA, the GTC, or any other applicable terms governing the use of the Cloud Services. Customers and Partners may not redistribute or publish the Documentation without Company's prior written consent, nor use the Documentation for any purpose that competes with Company's offerings or grant access to the Documentation to any competing company, understanding as such any entity that develops, markets, or distributes products or services similar or analogous to the Cloud Services.

7.3 **Feedback**. Partners and Customers are encouraged to provide feedback on the Documentation, including suggestions for improvement, reports of errors or omissions, and requests for additional topics. Feedback may be submitted to ciso-office@opinator.com.

8. THIRD-PARTY MATERIALS

8.1 **Included Third-Party Materials**. The Cloud Services may include or incorporate third-party software, libraries, frameworks, or other materials ("Third-Party Materials"). A list of Third-Party Materials and their applicable licenses is available upon request, provided that there is a valid agreement for the provision of Cloud Services in force.

8.2 **Third-Party Licenses**. Third-Party Materials are subject to their respective third-party licenses. Company grants no rights in Third-Party Materials beyond those granted by the applicable third-party licenses. Partners and Customers shall comply with all third-party license terms. Some Third-Party Materials may be subject to open source licenses that impose conditions on use, modification, or distribution.

8.3 **No Warranty for Third-Party Materials**. Company makes no representations or warranties regarding Third-Party Materials beyond those made by the respective third-party licensors. The limitations of liability and disclaimers in these GTC apply to Third-Party Materials to the maximum extent permitted by their licenses.

8.4 **Third-Party Services**. The Cloud Services may enable integration with or access to third-party services or platforms not provided by Company ("Third-Party Services"). Examples include:

(a) Single sign-on providers;

(b) Data import/export tools for external systems;

(c) Webhooks or APIs for connecting to external applications;

(d) Embedded content from third-party sources.

8.5 **Third-Party Service Terms**. Access to and use of Third-Party Services is subject to:

(a) The terms and conditions of the respective third-party provider;

(b) Any additional terms or limitations Company may impose;

(c) Customer's separate agreements with the third-party provider.

8.6 **Responsibility**. Company is not responsible for Third-Party Services and makes no warranties regarding their availability, functionality, security, or compliance with applicable laws.

8.7 **Changes to Third-Party Integrations**. Company may: (a) add new Third-Party Service integrations; (b) modify or discontinue support for existing Third-Party Service integrations; or (c) disable Third-Party Services that pose security risks or violate the Acceptable Use Policy. Company shall provide reasonable notice of material changes to Third-Party Service integrations.

9. UPDATES AND MODIFICATIONS TO GTC

9.1 **Right to Update**. Company reserves the right to update these GTC from time to time to reflect: (a) changes in Company's business practices or service offerings; (b) legal or regulatory requirements; (c) security enhancements; (d) customer feedback; or (e) changes to Third-Party Materials or Third-Party Services.

9.2 **Notice of Updates**. Company shall provide notice of updates to these GTC as follows:

(a) Material Changes: At least fifteen (15) days' prior notice to Partners and Customers via: (i) email to the notification addresses provided; and (ii) notice on the Cloud Services login page and/or posting the updated GTC at https://web.opinator.com/legal/partners/sales/gtc-resale.

(b) Non-Material Changes: Notice via posting the updated GTC at https://web.opinator.com/legal/partners/sales/gtc-resale. Non-material changes include corrections of typographical errors, clarifications that do not substantively change obligations, updates to contact information, and similar administrative changes.

(c) Material Changes Include: Changes that materially: (i) reduce Company's service levels or obligations; (ii) increase restrictions or obligations on Partners or Customers; (iii) reduce Company's liability or warranties; (iv) modify the Acceptable Use Policy to prohibit previously permitted activities; or (v) alter pricing structures or payment terms.

9.3 **Effective Date of Updates**. Updated GTC shall become effective:

(a) For New Orders: Immediately upon the effective date specified in the update notice;

(b) For Existing Orders: The later of: (i) thirty (30) days after notice of material changes; or (ii) upon renewal of the Subscription Term.

9.4 **Objection to Updates**. If Partner or Customer objects to a material update to these GTC:

(a) Partner or Customer must provide written notice of objection to Company within thirty (30) days of receiving notice of the update;

(b) The objection must specify the basis for the objection and which terms are unacceptable;

(c) The parties shall negotiate in good faith to resolve the objection;

(d) If resolution is not possible, Partner or Customer may terminate the affected services by providing written notice within the thirty (30) day objection period;

(e) Upon such termination, Company shall refund any prepaid fees for the terminated portion of the Subscription Term on a pro-rata basis;

(f) If no objection is received within the thirty (30) day period, the updates shall be deemed accepted.

9.5 **Emergency Updates**. Notwithstanding the foregoing notice requirements, Company may implement emergency updates to these GTC without prior notice if necessary to: (a) address an immediate security threat or vulnerability; (b) comply with law, court order, or regulatory requirement; or (c) prevent imminent harm to the Cloud Services or other customers. Company shall provide notice of emergency updates as soon as reasonably practicable.

9.6 **Version History**. Company maintains a version history of these GTC at https://web.opinator.com/legal/previous-versions, which shall include at least the two (2) most recent prior versions, plus any additional versions issued within the two (2) years preceding the current version.