DATA PROCESSING AGREEMENT

(« DPA »)

Last Revised: July 13, 2026

This Data Processing Agreement (hereinafter the "DPA") constitutes an annex to the SaaS Services Agreement (hereinafter the "Agreement").

Unless otherwise specifically stated in this DPA, CONFORMiT acts as a processor of personal data and the Client acts as a controller of personal data.

This DPA forms an integral part of the Cloud Service Agreement dated between the Parties and is governed by its terms, including those of this DPA. In accordance with Articles 1 and 14 below, in the event of any contradiction or inconsistency between the terms of the SaaS Services Agreement and this DPA, the DPA shall prevail over the content of the SaaS Services Agreement with respect to the processing of the Client's personal data by CONFORMiT and its subprocessors.

This DPA shall enter into force on the date of its signature by both Parties.

1. Introduction and Relationship with the Agreement

1.1 This DPA applies to all processing of Personal Data carried out by CONFORMiT and its Subprocessors in the context of the performance of the Agreement.
CONFORMiT shall process Personal Data only in accordance with the documented instructions of the Client, unless required to do so under the law to which it is subject (with prior notice to the Client unless legally prohibited). In the event of a conflict between this DPA and the Agreement, the provisions of this DPA relating to processing shall prevail, unless otherwise mandated by applicable Data Protection Law.
1.2 CONFORMiT shall immediately inform the Client if, in its opinion, an instruction given by the Client constitutes a violation of this DPA or of applicable data protection legislation. CONFORMiT may then suspend the performance of the Agreement. CONFORMiT may terminate the Agreement for cause attributable solely to the Client if the Client insists that its instructions be followed even though it has been informed by CONFORMiT that its instructions violate applicable legal requirements.
1.3 CONFORMiT processes the Client's personal data only for the specific purpose(s) of processing as defined in the Annex, unless otherwise instructed by the controller.
1.4 The processing of Client data by CONFORMiT shall take place only for the duration specified in the Annex.

2. Definitions

Capitalized terms not defined in this DPA have the meaning assigned in the Agreement. The following definitions apply:
« Standard Assistance » means the provision of information already available (policies, certifications, summaries) without significant customized work.
« Supervisory Authority » means any regulatory authority competent in data protection matters under applicable Data Protection Law.
« SCCs » (Standard Contractual Clauses): standard clauses adopted by the European Commission (Decisions 2021/914 and 2021/915).
« Anonymized Data » means data and information relating to the Client's use of the Services that has been irreversibly modified, in accordance with generally recognized practices, such that it is not possible at any time for a person to be identified directly or indirectly from such information, alone or in combination with other information, and which is used by CONFORMiT in an aggregated and

anonymized manner, including to compile statistical and performance information related to the provision and operation of the Services.

« Personal Data » means any information relating to an identified or identifiable natural person, as defined by applicable Data Protection Law.

« Client Data » means information, Personal Data, data and other content received from the Client through the Services. For clarity, Client Data does not include Anonymized Data.

« Security Incident » means a breach of security measures resulting in unauthorized access, use, disclosure, loss, alteration or destruction of Personal Data, meeting the notification criteria of applicable Data Protection Law.

The definition does not include unsuccessful attempts (failed logins, port scans, DDoS attacks) that do not compromise the security of Personal Data, including failed login attempts, port scans, denial of service attacks and other network attacks on firewalls or networked systems, except to the extent that such exclusion would conflict with the requirements of applicable Data Protection Laws.

« Applicable Data Protection Law » means all laws, regulations, ordinances, decrees, directives, binding guidelines, regulatory decisions and legally binding requirements relating to the protection of personal data, privacy, confidentiality of Personal Data, information security, or notification of data security breaches that are applicable to the Processing carried out under this Agreement according to the territorial, material and personal application criteria specific to each of these laws, including: (a) European Union and European Economic Area data protection laws, including Regulation (EU) 2016/679 ("GDPR") and European national transpositions; (b) Canadian federal, provincial and territorial laws on the protection of Personal Data in the private sector, including An Act respecting the protection of personal information in the private sector, CQLR, c. P-39.1, ("Bill 25"), and the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA"); (c) U.S. federal and state consumer privacy and data breach notification laws (CCPA/CPRA and others); (d) United Kingdom data protection laws, including the UK GDPR; (e) the Swiss FADP; (f) any other law, regulation or binding requirement relating to data protection or privacy that becomes applicable to the Processing by virtue of its own provisions relating to its scope and criteria.

This definition does not constitute a voluntary submission of the Parties to any law that would not otherwise apply to the Processing under its own territorial, material or personal application rules.

« Swiss FADP » means the Swiss Federal Act on Data Protection of 25 September 2020, as amended.

« Data Subject » means the identified or identifiable natural person to whom the Personal Data of the applicable Data Protection Law relates.

« Sensitive Information » means sensitive Personal Data which, due to its nature, including medical, biometric, genetic or otherwise intimate, or due to the context of its use or disclosure, raises a high degree of privacy concern, as defined by applicable Data Protection Law. This definition includes genetic, biometric and health data within the meaning of Regulation (EU) 2016/679 ("GDPR") and sensitive data within the meaning of the Standard Contractual Clauses approved by Implementing Decisions (EU) 2021/914 and 2021/915.

« Subprocessor » means any third party engaged by CONFORMiT to process Personal Data on behalf of the Client as described in Annex C of the DPA.

« Processing »: has the meaning given in applicable Data Protection Law.

« UK IDTA » means the United Kingdom International Data Transfer Agreement or the UK Addendum to the EU SCCs, issued by the Information Commissioner's Office under section 119A(1) of the Data Protection Act 2018.

3. Scope of Processing

The subject matter, duration, nature, purpose of the processing, the types of Personal Data and the categories of Data Subjects are set out in the Annex hereto. International transfers are governed by Annex B.

4. Obligations of the Parties

4.1 Obligations of CONFORMiT

4.1.1 Instructions: The Client shall provide clear, complete and documented instructions to CONFORMiT. CONFORMiT may only process the Client's Personal Data in accordance with the instructions provided by the Client, and for the specific purpose(s) of processing provided. Any additional instructions shall be documented in writing and may incur additional Professional Services fees.

4.1.2 Security: CONFORMiT shall take all technical and organizational measures appropriate to the risks, in accordance with Article 32 of the GDPR, including in particular: pseudonymization and encryption, ensuring constant confidentiality/integrity/availability and resilience of systems, ability to restore after an incident, and regular effectiveness testing. The security measures are described in the Annex hereto and shall be reviewed at least annually or in the event of a major change.

The Parties acknowledge that these technical and organizational measures are designed to ensure a level of protection appropriate to the identified risks and to meet legal information security requirements taking into account the nature of the processing and the information available to CONFORMiT.

4.1.3 Assistance: In accordance with applicable Data Protection Law, CONFORMiT shall provide Assistance for: (i) data protection impact assessments (DPIA/PIA); (ii) consultations with Supervisory Authorities; (iii) regulatory investigations, inquiries, security obligations. The Client shall reimburse excess costs at Professional Services rates.

4.1.4 Data Subject Rights: CONFORMiT shall assist the Client in responding to requests to exercise rights (access, rectification, erasure, restriction, portability, objection, and not to be subject to a decision based solely on automated processing, to the extent required by applicable Data Protection Law according to its own application criteria). This assistance is limited to Standard Assistance.

The Client shall reimburse additional costs related to third party requests.

4.1.5 Register: CONFORMiT shall maintain a register of processing activities in accordance with applicable Data Protection Law.

4.1.6 Confidentiality: CONFORMiT shall ensure that persons authorized to process personal data are bound by confidentiality undertakings or are subject to an appropriate statutory obligation of confidentiality.

4.1.7 Deletion: CONFORMiT shall delete or return to the Client all personal data at the end of the provision of services relating to processing under the conditions set out in Article 12 hereof.

4.1.8 Compliance: CONFORMiT shall make available to the Client all information necessary to demonstrate compliance with the obligations provided for by applicable Data Protection Law and to allow audits by the Client to be carried out under the conditions described in Article 10 hereof.

4.1.9 Processor Register : CONFORMiT undertakes to maintain a register of all categories of processing activities carried out on behalf of the Client, including: the name and contact details of the controller on whose behalf it acts, any Subprocessors and, where applicable, the data protection

officer; the categories of processing carried out on behalf of the controller; where applicable, transfers of personal data to a third country or international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49(1), second subparagraph, of the GDPR, documents attesting to the existence of appropriate safeguards; where possible, a general description of the technical and organizational security measures, including, inter alia, as necessary: the pseudonymization and encryption of personal data, means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, means to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident, a procedure for regularly testing, analyzing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing. CONFORMiT shall make this register available to the Client upon first request.

4.2 Obligations of the Client

4.2.1 The general obligations of the Client are set out in the Agreement. The Client must: respond to requests from Data Subjects and Supervisory Authorities; notify CONFORMiT of any change in the purposes of processing; cooperate for any clarification; make notifications in the event of a Security Incident, in accordance with applicable Data Protection Law.

4.2.2 The Client warrants that its instructions to CONFORMiT regarding the use of Personal Data will comply with applicable Data Protection Laws. CONFORMiT ensures that the processing of Personal Data it carries out complies with applicable Data Protection Laws and is not responsible for claims arising from non-compliant instructions from the Client.

4.2.3 Fees: The Client agrees to pay additional fees resulting from modifications to its instructions, unless motivated by a change in applicable Data Protection Laws or instructions from the competent Supervisory Authority.

4.3 U.S. Provisions

When U.S. Data Protection Laws apply to the Processing, CONFORMiT as a service provider or "processor" within the meaning of such laws shall (a) not sell or share Personal Data; (b) use it only for the purposes specified in the Agreement or otherwise permitted by applicable Data Protection Law; (c) not combine it with other sources, unless permitted by law.

5. Security Incidents

5.1 Notification: CONFORMiT shall notify the Client of any Security Incident without undue delay, and no later than 72 hours after becoming aware of it. CONFORMiT's notification obligation takes effect from the time it actually becomes aware of a confirmed Security Incident, and not from the mere detection of a technical anomaly. The Client remains responsible for notifications to Data Subjects and Supervisory Authorities.

5.2 Content: The notification shall include, as available: the nature of the incident, the approximate categories and numbers of Data Subjects, the contact details of the point of contact, the likely consequences, and remediation measures. CONFORMiT may provide this information progressively. The notification does not constitute an acknowledgment of liability.

5.3 Register: CONFORMiT shall provide the information necessary for the register of incidents as part of Standard Assistance.

5.4 Third Party Notification: CONFORMiT shall not inform any third party of a Security Incident without the prior written consent of the Client, except where required by applicable Data Protection Laws or other laws or regulations.

5.5 Exclusion: If an Incident results from the Client's instructions, negligence, willful breach or violation, the Client shall bear the costs of investigation, notification and remediation.

6. Confidentiality

Confidentiality obligations are governed by the Agreement. CONFORMiT undertakes to ensure that persons authorized to process Personal Data undertake to respect confidentiality or are subject to an appropriate statutory obligation of confidentiality, and have received appropriate training.

7. Subprocessors

7.1 The list of Subprocessors is set out in Annex C. The Client grants general authorization to CONFORMiT to engage Subprocessors. CONFORMiT shall inform the Client of any change with 30 days' notice. The Client shall have 15 business days to raise a written objection supported by documented legitimate reasons. In the event of a legitimate and documented objection, the Parties shall consult in good faith to find a mutually acceptable solution.

7.2 CONFORMiT shall impose on its Subprocessors substantially equivalent obligations and remains responsible for their acts and omissions to the extent that they result from CONFORMiT's failure to impose such obligations or to exercise supervision.

7.3 For transfers to third countries without an Adequacy Decision, CONFORMiT shall ensure that appropriate safeguards (SCCs Module 3 or equivalent) are in place.

7.4 Where the Client designates a specific Subprocessor, CONFORMiT assumes no responsibility for the acts or omissions of that designated Subprocessor beyond CONFORMiT's control.

8. International Transfers

8.1 CONFORMiT is authorized to transfer Personal Data to the countries and entities identified in Annex C, subject to appropriate safeguards. The applicable transfer mechanisms are detailed in Annex B.

8.2 CONFORMiT shall comply with its legal obligations. To the extent permitted by applicable data protection laws, CONFORMiT shall inform the Client of any request affecting Personal Data.

8.3 Transfer Impact Assessments (TIA): The Client assumes responsibility for determining whether a TIA is required. CONFORMiT shall provide, upon request and for compensation, available information, subject to the protection of its trade secrets and its obligations to other clients. If a TIA reveals inadequacy of the SCCs, the Parties shall collaborate to identify additional measures in accordance with EDPB Recommendations 01/2020.

9. Data Protection Officer

CONFORMiT shall appoint a data protection officer in accordance with applicable Data Protection Law.

Contact: privacy@conformit.com
Physical address: CONFORMiT Technologie Inc., 125 rue Dubé (Bureau 200), Chicoutimi (Québec) G7H 2V3

10. Audits

10.1 CONFORMiT shall provide the Client with its current certifications (SOC 2 Type II, ISO 27001, ISO 27017 or equivalent), which constitute prima facie evidence of compliance and satisfy the audit obligations of applicable Data Protection Law.

10.2 The Client may, upon 30 days' notice and at its own expense, commission a limited audit of 5 business days, once per year, unless: (a) required by a Supervisory Authority; (b) a Security Incident has occurred; or (c) CONFORMiT has not provided a third-party report.

10.3 Any audit must be conducted during business hours; be subject to a confidentiality agreement; not interfere with operations; be coordinated with audits of other clients where possible to minimize disruption; be limited to systems related to the Client's processing. CONFORMiT shall invoice audit costs exceeding the review of existing reports.

10.4 Audits must not compromise trade secrets, security architectures, obligations to other clients, or the security of CONFORMiT's infrastructure.

10.5 CONFORMiT may object to an auditor who is a competitor or creates a conflict of interest. In the event of an objection, the Client shall propose an acceptable alternative auditor.

11. Limitation of Liability

11.1 The limitations of liability of the Agreement apply to this DPA, subject to the mandatory provisions of applicable Data Protection Law. In accordance with Article 82(4) of the GDPR, no limitation applies to liability towards Data Subjects where contrary to the GDPR.

11.2 CONFORMiT's aggregate liability for claims arising out of this DPA is subject to the cap established in the Agreement.

11.3 CONFORMiT shall not be liable for fines or administrative penalties imposed on the Client by a Supervisory Authority, unless resulting directly and exclusively from a demonstrated breach by CONFORMiT of its own obligations under applicable Data Protection Law.

12. Return and Deletion of Data

12.1 Upon termination or expiration of the Agreement, CONFORMiT must, at the Client's choice notified within 30 days: (a) return the Personal Data within 90 days at the Client's expense; fees shall be determined based on time and materials; or (b) securely delete or destroy them at no cost. In the absence of a choice notified by the Client within the prescribed period, CONFORMiT shall proceed with deletion. CONFORMiT shall provide a certificate of deletion upon request.

12.2 CONFORMiT may retain Personal Data: in standard backups (up to 90 days after operational deletion); as required by law or for legitimate purposes (accounting, actual or pre-litigation disputes, compliance); in system logs (up to 180 days). Such data remains protected by this DPA.

12.3 Any retention of Personal Data under this article shall be limited to what is strictly necessary for the aforementioned purposes and such Personal Data shall remain subject to the security and confidentiality obligations set out in this DPA.

12.4 This article applies only to Personal Data processed on behalf of the Client and not to information that CONFORMiT processes as an independent controller.

13. Survival

The following Articles shall survive the expiration or termination of this Agreement or any part thereof: 2 (Definitions), 5 (Security Incidents), 6 (Confidentiality), 8.2 (Government Access Requests), 11 (Limitation of Liability), 12 (Return and Deletion of Data), 13 (Survival), and 14 (General Provisions).

14. General Provisions

14.1 Hierarchy: In the event of a conflict, the following order of precedence applies: (1) Mandatory provisions of applicable Data Protection Law; (2) SCCs or equivalent transfer mechanisms; (3) UK IDTA/Addendum; (4) Annexes to this DPA; (5) Main body of the DPA; (6) Agreement and its other annexes, according to the order of precedence established in the Agreement.

14.2 Amendments: This DPA may only be amended in writing signed by both Parties, except that CONFORMiT may update the Annexes (with notification).

ANNEX A – Processing Details

Duration

This DPA shall remain in effect for the entire duration of the SaaS Agreement and as necessary for clauses that survive it.

Nature of Processing Carried Out by CONFORMiT for the Client:

- Data collection
- Data recording
- Data organization
- Data structuring
- Data storage
- Data adaptation or modification
- Data extraction
- Data consultation
- Data use
- Data disclosure (transmission or any other form of making available)
- Data matching
- Data interconnection
- Data restriction
- Data erasure
- Data destruction

Purpose of Processing:

- Provision of Services described in the Agreement
- Technical assistance and customer support
- Service improvement
- Security and fraud prevention
- Management of the business relationship
- Marketing and communication

Categories of Personal Data:

- Employee data (names, contact information, identifier)
- Occupational health and safety incident data
- Compliance audit data

Categories of Data Subjects

Client employees.

Technical and Organizational Measures

CONFORMiT shall implement, to the extent commercially reasonable taking into account the state of the art, implementation costs and risks to data subjects, the following security measures:

Access Control: Multi-factor authentication; role-based controls; annual reviews; immediate revocation upon termination of employment.

Encryption: In transit (TLS 1.2+); at rest (AES-256 or equivalent).

Physical and Network Security: Logging and monitoring; environmental controls; firewall and IDS/IPS; annual vulnerability scans and penetration testing; network segmentation.

Organizational Measures: Security policies and procedures; annual training; background checks; incident response plan.

Continuity: Regular backups; disaster recovery plan; annual recovery testing.

Monitoring: Security logging; annual third-party audits (SOC 2 Type II or equivalent); regular testing.

ANNEX B – International Transfers and Subprocessors

C.1 Transfer Mechanisms

From	To	Mechanism
EEA	Canada	Adequacy Decision (PIPEDA) or SCCs Module 2
EEA	United States	DPF (if certified) or SCCs Module 2 with TIA
UK	Third countries	UK IDTA or UK Addendum to SCCs
Switzerland	Third countries	Adapted SCCs (FDPIC) or Swiss-US DPF
Quebec	Outside Quebec	PIA required (art. 17 Bill 25); this DPA = written agreement
Canada	Third countries	Principle 4.1.3 PIPEDA; contractual agreement

C.2 Transfers from the European Economic Area (EEA)

C.2.1 Incorporation of SCCs. To the extent that CONFORMiT processes Personal Data from the EEA and an international transfer mechanism is required under the GDPR, the Parties agree to execute the European Commission's Standard Contractual Clauses (Decision 2021/914) as follows:

(a) Module 2 (Controller to Processor) applies where the Client is the data exporter located in the EEA acting as controller and CONFORMiT is the data importer acting as processor;
(b) Module 3 (Processor to Processor) applies where the Client itself acts as a processor for a third-party controller;
(c) Annexes I to III of the SCCs are completed by reference to the information contained in Annex A and section C.7 of this DPA.

C.2.2 Optional Clauses. The Parties agree that: (a) Clause 7 (Docking clause) applies; (b) for Clause 9(a), Option 2 (general written authorization) applies with a notice period of thirty (30) days; (c) Clause 11(a) (optional dispute resolution clause) does not apply; (d) for Clause 17, the laws of the French Republic apply; (e) for Clause 18, the courts of the Client's seat established in the French Republic have jurisdiction.

C.3 Transfers from the United Kingdom

C.3.1 Incorporation of UK IDTA. To the extent that CONFORMiT processes Personal Data from the United Kingdom and an international transfer mechanism is required under the UK GDPR, the UK International Data Transfer Addendum to the EU SCCs (or the standalone UK IDTA) is incorporated by reference.
C.3.2 Modifications. References to the EU, Member States and the GDPR in the SCCs are modified mutatis mutandis to refer to the United Kingdom, the Data Protection Act 2018 and the Information Commissioner's Office (ICO). For Clause 17, the laws of England and Wales govern. For Clause 18, the courts of London, England have jurisdiction.

C.4 Transfers from Switzerland

C.4.1 To the extent that CONFORMiT processes Personal Data from Switzerland and an international transfer mechanism is required under the Swiss FADP, the EU SCCs apply with the following modifications: (a) references to the GDPR are interpreted as references to the Swiss FADP; (b) references to "Member State" are interpreted as including Switzerland; (c) the competent supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC); (d) the SCCs are governed by Swiss law; (e) the competent courts are the Swiss courts.

C.5 Transfers from Quebec and Canada

C.5.1 PIA Required. The Client assumes sole responsibility for conducting any PIA required under section 17 of Bill 25 prior to any transfer of Personal Data outside Quebec. The PIA must take into

account: (a) the sensitivity of the information; (b) the purposes for which it will be used; (c) the applicable protective measures; (d) the legal framework applicable in the State to which the information will be disclosed.
In accordance with section 17 of Bill 25, this DPA constitutes the required written agreement between the Client and CONFORMiT for transfers of Personal Data outside Quebec, which provides for: (i) the applicable protective measures set out in Article 4.1.2; (ii) the limits on the use of information established in Articles 1 and 3; and (iii) the Client's right to verify these measures in accordance with Article 10.
C.5.2 CONFORMiT Assistance. CONFORMiT shall provide, as part of the Standard Assistance defined in Article 4.1.3, general information about its security practices and the location of its Subprocessors. Any additional assistance, including review of specific PIAs, shall be billed at current Professional Services rates.
C.5.3 Canada's Adequacy Status. The Parties acknowledge that Canada benefits from an Adequacy Decision from the European Commission (Decision 2002/2/EC, reaffirmed in 2024) for organizations subject to PIPEDA, thereby facilitating transfers from the EEA to Canada for covered entities.

C.6 Transfers to the United States

C.6.1 EU-U.S. Framework. To the extent that CONFORMiT or its Subprocessors are certified under the EU-U.S. Data Privacy Framework, transfers to such entities may be made on the basis of such certification, subject to verification by the Client of active certification.
C.6.2 SCCs as Alternative Mechanism. In the absence of DPF certification or where required, the SCCs apply in accordance with section C.2.

C.7 Standard Contractual Clauses Framework

C.7.1 Incorporation. The European Commission's Standard Contractual Clauses (Implementing Decision (EU) 2021/914) are incorporated by reference into this DPA for transfers requiring such a mechanism.
C.7.2 Applicable Modules

- Module 2 (Controller to Processor): applies when the Client is the controller and CONFORMiT is the processor.
- Module 3 (Processor to Processor): applies when the Client itself acts as a processor for a third-party controller.

C.7.3 Information for Annex I of the SCCs (Parties and Transfer).

- Data exporter: The Client (contact details in the Agreement)
- Data importer: CONFORMiT Technologie Inc., 125 rue Dubé (Bureau 200), Chicoutimi (Québec) G7H 2V3, Canada
- Data protection contact: privacy@conformit.com
- Description of transfer: As described in Annex A of this DPA

C.7.4 Information for Annex II of the SCCs (Technical and Organizational Measures). The measures are those described in the Annex to this DPA.
C.7.5 Competent Supervisory Authority (Annex I.C of the SCCs). The competent supervisory authority is determined in accordance with Clause 13 of the SCCs. In case of doubt, the Commission d'accès à l'information du Québec (CAI) is the lead authority for matters under Bill 25, and the authority of the data exporter's Member State for matters under the GDPR.
C.7.6 UK Addendum. The UK International Data Transfer Addendum to the EU SCCs (version of 21 March 2022) is incorporated by reference for transfers from the United Kingdom. Tables 1 to 4 of the UK Addendum are completed by reference to this DPA.
C.7.7 Swiss Modifications. For transfers from Switzerland, the modifications provided in section C.4 apply to the SCCs.

Annex C —Subprocessors

This Annex identifies the Subprocessors authorized to process Personal Data on behalf of the Client in the context of the provision of Services.

NAME	SERVICE	LOCATION	CONFORMiT SERVICES	APPLICABLE TO	DATA TYPE
Amazon Web Services (AWS)	Cloud Hosting and AI Cloud Services	Canada	Application, Platform	All customers worldwide	• EHS Data Identity (First • Name, Last Name) • Contact Information (Email)
SendGrid (Twilio)	Transactional Email Delivery	United States	User Notifications	All customers worldwide	• Identity (First Name, Last Name) • Contact Information (Email)
Zoho Corporation	Enterprise Resource Planning (ERP), Business Management	United States	• Billing Support • Services • Ideas/Feedback Portal • Communication, Customer Relations	All customers worldwide	• Billing Data Support • Tickets Bug • Reports Feature • Requests Customer • Contact Information
Microsoft Azure	AI Cloud Services	Canada	Artificial Intelligence Services, Johnny (EHS.ai)	All customers using Johnny (EHS.ai)	• Queries and interactions with Johnny AI Assistant (EHS.ai)
HubSpot	Customer Relationship Management (CRM)	United States	Commercial Terms, SOW, Contracts, Agreements	All customers worldwide	• Business information related to Statements of Work (SOW)