Published on October 11, 2024.

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is made by and between SANGOMA TECHNOLOGIES INC. ("**Sangoma**") and Customer in accordance with the Master Agreement entered into by the Parties.

Sangoma and Customer may be referred to collectively as the "**Parties**" and individually as a "**Party**." Capitalized terms not otherwise defined in this DPA shall be as defined in the Master Agreement.

RECITALS

1. Customer and Sangoma entered into an agreement for Sangoma to provide Services to Customer ("**Master Agreement**").

2. To comply with its obligations under the Master Agreement, Sangoma may need to process Personal Data provided by or collected for Customer.

3. This DPA sets out the additional terms, requirements, and conditions on which Sangoma will obtain, handle, process, disclose, transfer, or store Personal Data when providing Services under the Master Agreement.

AGREEMENT

The Parties agree as follows:

1. Recitals. The recitals stated above are true and hereby incorporated and made part of this DPA.

2. Definitions and Interpretation

2.1 Definitions:

"**Customer**" is the party that entered into the Master Agreement with Sangoma, which incorporates this DPA by reference.

"**Data Subject**" means an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.

"**Data Privacy Framework**" means the EU-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.

"**EU Data Protection Law**" means all data protection laws and regulations applicable to European Economic Area, including (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (b) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (c) applicable national implementations of (a) and (b).

"**Personal Data**" means any information Sangoma processes for Customer that (1) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Sangoma's possession or control or that Sangoma is likely to have access to, or (2) the relevant Privacy and Data Protection Requirements otherwise define as "protected personal data," "personally identifiable information," "personal information," or other similarly defined information.

"**Processing, processes, and process**" means any activity that involves the use of Personal Data, or as the relevant Privacy and Data Protection Requirements may otherwise define the terms processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

"**Privacy and Data Protection Requirements**" means all applicable laws and regulations relating to the processing, protection, or privacy of the Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, the EU Data Protection Law, and the UK Data Protection Law.

"**Sangoma Affiliate**" means Sangoma affiliates, subsidiaries, or sister companies (companies controlled by the same parent company) that may assist in the performance of the Services or this DPA, and may be engaged in the processing of Personal Data.

"**Security Breach**" means a breach of Sangoma's security leading to the accidental or unlawful loss, destruction, alteration, or unauthorized disclosure of, or access to, Personal Data on systems managed by or otherwise controlled by Sangoma.

"**Services**" means all services provided by Sangoma in accordance with the Master Agreement.

"**Standard Contractual Clauses (SCC)**" means the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries (Module Two), as set out in the Annex to Commission Decision (EU) 2021/914, a completed copy of which comprises Annex B.

"**Sub-processor**" means any Sangoma Affiliate and any sub-contractor engaged by Sangoma that will process Personal Data in connection with the Services.

"**UK Data Protection Law**" means all data protection laws and regulations applicable to the United Kingdom, including (a) the Data Protection Act 2018 and (b) the GDPR, as incorporated into the United Kingdom law under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**").

2.2 This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this DPA.

2.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

2.4 A reference to writing or written includes email.

2.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail;

(c) any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail; and

(d) any of the provisions of this DPA and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

3. Personal Data Types and Processing Purposes

3.1 The Parties acknowledge that for the purpose of any applicable Privacy and Data Protection Requirements, Customer is the data controller and Sangoma is the data processor.

3.2 Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Sangoma.

3.3 Customer represents and warrants that it has (a) complied, and will continue to comply with Privacy and Data Protection Requirements, in respect of its processing of Personal Data and any processing instructions it issues to Sangoma; and (b) provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Privacy and Data Protection Requirements for Sangoma to Personal Data for the purposes described in the Master Agreement.

3.4 Annex C describes the general Personal Data categories and Data Subject types Sangoma may process in fulfilling the Services.

4. Provider's Obligations

4.1 Sangoma will only process the Personal Data to the extent, and in such a manner, as is necessary for the Services, in accordance with this DPA, and Customer’s documented, lawful instructions. Sangoma will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Privacy and Data Protection Requirements. Sangoma must promptly notify Customer if, in its opinion, Customer's instruction does not comply with the Privacy and Data Protection Requirements.

4.2 Except as required by applicable law, Sangoma will promptly comply with any Customer request or instruction requiring Sangoma to amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized processing.

4.3 Sangoma will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless Customer, the Master Agreement or this DPA specifically authorizes the disclosure, or as required by law. If a law requires Sangoma to process or disclose Personal Data, Sangoma must first inform Customer of the legal requirement and give Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

4.4 Sangoma will reasonably assist Customer with meeting Customer's compliance obligations under the Privacy and Data Protection Requirements, while also considering the nature of Sangoma's processing and the information available to Sangoma, provided that (a) Customer is unable to meet such compliance obligations without Sangoma’s assistance, and (b) Sangoma is legally permitted to provide such assistance.

5. Security

5.1 Sangoma must at all times implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, unavailability, destruction, or damage.

5.2 Sangoma must take reasonable precautions to preserve the integrity of any Personal Data it processes and to prevent any corruption or loss of the Personal Data, including but not limited to establishing effective back-up and data restoration procedures.

5.3 Upon Customer's written request, Sangoma will make all the of the relevant audit reports available to Customer for review.

5.4 Sangoma has implemented and will maintain appropriate measures to ensure that all employees and contractors involved in the processing of Personal Data are authorized personnel with a need to access the Personal Data, are bound by appropriate confidentiality obligations, and have undergone appropriate training in the protection and handling of Personal Data.

6. Security Breach and Personal Data Loss

6.1 Sangoma will without undue delay (a) notify Customer if it becomes aware of any Security Breach, and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach.

6.2 In the event of a Security Breach, Sangoma shall provide Customer with all reasonable assistance in dealing with the Security Breach, in particular in relation to making any notification to a supervisory authority or any communication to a Data Subject. Sangoma will reasonably cooperate with Customer in Customer's handling of the matter.

7. Cross-Border Transfers of Personal Data

7.1 If the Privacy and Data Protection Requirements restrict cross-border Personal Data transfers, Customer will only transfer that Personal Data to Sangoma under the following conditions:

(a) Sangoma, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, may legally receive that Personal Data. Sangoma must identify in Annex A the location or mechanism that enables it to receive that Personal Data and must immediately inform Customer of any change to that status;

(b) Customer obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements; or

(c) The transfer otherwise complies with the Privacy and Data Protection Requirements for the reasons set forth in Annex A.

7.2 If any Personal Data transfer between the Parties requires execution of Standard Contractual Clauses in order to comply with the Privacy and Data Protection Requirements, the Parties will complete all relevant details in, and execute, the Standard Contractual Clauses contained in Annex B, and take all other actions required to legitimize the transfer, including implementing any needed supplementary measures or supervisory authority consultations.

7.3 Sangoma will not transfer any Personal Data to another country unless the transfer complies with the Privacy and Data Protection Requirements.

7.4 To the extent that Sangoma is the recipient of Personal Data governed by UK Data Protection Law in a country that is not recognized as providing an adequate level of protection for Personal Data as described in UK Data Protection Law, the Parties shall:

(a) rely on the Data Privacy Framework as a legal basis for transfers of Personal Data in the United States, in compliance its data privacy principles; or

(b) when the Data Privacy Framework is not applicable or is invalid under the Privacy and Data Protection Requirements, abide by the United Kingdom International Data Transfer Addendum set forth in Annex E.

8. Sub-Processor

8.1 Sangoma may engage a Sub-processor to (i) assist Sangoma in carrying out the Services, or (ii) provide certain services to Sangoma.

8.2 Sangoma shall maintain a written agreement with each Sub-processor that contains data protection obligations not less protective than those in this DPA, with respect to the protection of Personal Data. If a Sub-processor fails to fulfil its obligations under such written agreement, Sangoma remains fully liable to Customer for such Sub-processor's performance of its obligations under such written agreement.

8.3 Sangoma currently utilizes the Sub-processors set forth in Annex F, which are authorized by Customer.

9. Complaints and Data Subject Rights Requests

9.1 Sangoma will, to the extent legally permitted, promptly notify Customer if it receives any complaint, notice, or communication related to the processing of the Personal Data or to either Party's compliance with the Privacy and Data Protection Requirements.

9.2 If Sangoma receives such a request in relation to Personal Data, Sangoma will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request. For the avoidance of doubt, Sangoma shall *not* be obligated to grant a request where the Data Subject is not entitled to the relief sought.

9.3 Sangoma shall, at the request of Customer, assist Customer, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a data subject request under the Privacy and Data Protection Requirements and/or in demonstrating such compliance, where possible.

10. Term and Termination

10.1 This DPA will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) Sangoma retains any Personal Data related to the Master Agreement in its possession or control ("**Term**").

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Data will remain in full force and effect.

11. Data Return and Destruction

11.1 Except as required otherwise by applicable law, Sangoma will update, correct, or delete Personal Data upon on Customer's request,

11.2 Except as required otherwise by applicable law, upon both the termination of the Master Agreement and the request by Customer, Sangoma shall delete or return to Customer all the Personal Data in its possession or control.

11.3 Upon Customer's request, Sangoma shall provide a portable copy of the Personal Data in accordance with the Privacy and Data Protection Requirements.

11.4 Any costs incurred by Sangoma arising from Sections 11.1 to 11.3 shall be borne by Sangoma. Any further costs incurred by Sangoma arising from Customer's specific requests that are different from the ones described in Sections 11.1 to 11.3 shall be borne by Customer.

12. Records

12.1 Sangoma shall maintain complete, accurate, and up to date written records of all Processing activities carried out on behalf of Customer containing information as required under any applicable Privacy and Data Protection Requirements("**Records**").

12.2 Sangoma will ensure that the Records are sufficient to enable Customer to verify Sangoma's compliance with its obligations under this DPA.

13. Liability Limitations

13.1 Each Party and all of its affiliates' liability, taken in the aggregate and arising in connection with this DPA, shall be subject to the exclusions and limitations of liability set forth in the Master Agreement.

14. Notice

14.1 Any notice or other communication given to a Party under or in connection with this DPA must be in writing and delivered to:

(a) For Customer: As provided for by Customer in the quote, order form, or similar documentation as amended from time to time as instructed by Customer in writing.

(b) For Sangoma: legal@sangoma.com

14.2 Section 14.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

Annex A

Personal Data Processing Purposes and Details

Sangoma's legal basis for receiving Personal Data with cross-border transfer restrictions:

☒ Located in an EEA Member State or in a country with a current determination of adequacy (list country): Canada, United Kingdom, Ireland

☐ Binding Corporate Rules (BCRs)

☒ Standard Contractual Clauses (SCCs)

☐ Other (describe in detail): _____

Annex B

Standard Contractual Clauses

See as published at https://sangoma.com/legal/.

Annex C

Personal Data Processing Purposes and Details

Categories of data subjects whose personal data is transferred

- Customer's personnel; Customer's customers

Categories of personal data transferred

- Names; phone numbers; call record details; payment information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- No sensitive data will be transferred from the data exporter to the data importer.

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

- The frequency of the transfer will be on a continuous basis.

Nature of the processing

- The nature of the processing of Personal Data is to provide the Services.

Purpose(s) of the data transfer and further processing

- Sangoma will process Personal Data as necessary to perform the Services, as specified in the DPA, and as further instructed by Customer in its use of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- The Term and the period from expiry of the Term until deletion of all Personal Data by Sangoma in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- The subject matter and nature of the processing by Sub-processors are specified in Annex A of the DPA. The duration of the processing carried out by Sub-processors will be until Sangoma stops processing the Personal Data.

Published on October 11, 2024.

Annex D

Security Measures

Sangoma and its affiliates maintain rigorous cybersecurity standards and technology control capabilities designed to protect both our and our customer's information in our care in a constantly evolving threat landscape. Our abilities combine best practices to promote the secure delivery of our services, assess and safely adopt emerging technologies to support those services, and meet regulatory requirements where we operate. Sangoma takes its role as a globally significant communications and services provider seriously and contributes to international initiatives that safeguard critical infrastructure and the global security landscape. Sangoma remains committed to protecting and supporting our clients and enhancing their awareness of security risks, with the ultimate goal of building a safe and resilient partner ecosystem.

How Our Capabilities Are Designed

Our Policies and Standards provide the foundation for our capabilities and approach to safeguard our technology environment. Coverage extends to applications, infrastructure, data, and facilities, which is designed to:

- Provide for the security, confidentiality, and availability of customer and employee information.
- Protect against anticipated threats or risks to the security or integrity of that information
- Prohibit unauthorized access to, or use of, information that could harm any customer, client, or employee
- Effectively manage, store, transport, and dispose of customer, client, and employee information
- Require our third-party service providers to adhere to the level of our security Policies and Standards in accordance with applicable regulatory obligations
- Provide our employees with the necessary awareness and training on their responsibilities to protect customer and client information and maintain the security of our systems

How Cybersecurity And Technology Are Governed

The infrastructure and security teams are overseen by the CISO in coordination with the CIO and Legal groups. Designed to monitor, report, and escalate the status of information and cybersecurity risks, this structure uses key forums to disseminate management information; monitor and measure progress; maintain compliance. These forums are established at multiple levels throughout the organization.

How We Implement Cybersecurity And Technology Controls

Sangoma's framework enables a systematic and consistent identification, control, and management of cybersecurity-related risks in a manner consistent with the company's risk tolerance.

Controls

Sangoma attempts to establish the controls necessary to meet business objectives. The protection of technology resources from unauthorized access, disclosure, modification, disruption, or destruction is essential in assuring the confidentiality, integrity, and availability of the information used within our processes. As such, technology controls are critical to securely and reliably service our clients.

Alignment With Industry Standards And Regulations

The Policies and Standards are subject to periodic inspection by third parties for compliance with, but not limited to:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Service Organization Control Type 2 (SOC2)

Assess And Measure Risk

Sangoma assesses and evaluates the adequacy of controls via automated or manual processes. Continuous monitoring for the control effectiveness is performed to determine the effectiveness and alignment of those controls. Control objectives are measured against the standards and business needs of the organization.

Risk Treatment

Sangoma monitors and manages risk exposure through communication with appropriate personnel and prioritized remediation. Issues resulting from a control gap or weakness identified by internal or third party sources are addressed promptly and escalated internally as appropriate.

Customer Inquiries

Sangoma will respond to customer and data subject inquiries concerning the security and privacy of its products and services.

Annex E

United Kingdom International Data Transfer Addendum

To the extent that Sangoma is the recipient of Personal Data governed by UK Data Protection Law in a country that is not recognized as providing an adequate level of protection for Personal Data as described in the UK GDPR, the Parties agree to abide by the Standard Contractual Clauses set forth in Annex B of the DPA together with the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, in force 21 March 2022) available at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf as may be amended, superseded, or replaced ("**UK Addendum**").

The UK Addendum is incorporated into the DPA by reference, and the execution of the DPA is deemed to constitute execution of the UK Addendum. The UK Addendum is deemed completed as follows:

(1) Table 1 will be populated by the information in the DPA. For the avoidance of doubt, Sangoma is acting as the importer and Customer is acting as the exporter.

(2) Table 2: The Parties agree the UK Addendum is appended to the Standard Contractual Clauses set forth in Annex B of the DPA.

(3) Table 3 is completed as follows:

(i) Annex 1A: List of Parties: As set forth in the DPA.

(ii) Annex 1B: Description of Transfer: As set forth in Annex C of the DPA.

(iii) Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex D of the DPA.

(iv) Annex III: List of Subprocessors (Modules 2 and 3 only): As set forth in Annex A of the DPA.

(4) Table 4: Which Parties may end the UK Addendum as set out in its Section 19: neither Party.

Published on October 11, 2024.

Annex F

Approved Sub-Processors

Company	Description of the Processing	Data Processed	Processing Locations	Applicable Sangoma Services
Voicebooth, dba Billingbooth	Process CDRs (Call Detail Records) in order to create the monthly invoice.	CDRs Payment Information	United Kingdom	Switchvox Cloud, Switchvox as a Service, SIPStation, PBXact Cloud
Simwood	Process live calls and post call generate CDRs for the purpose of billing.	CDRs	United Kingdom	Switchvox Cloud, SIPStation, PBXact Cloud
Amazon Web Services	Service provider (IaaS/PaaS/SaaS) for application data storage and processing required to support Sangoma's services.	System access information	United Kingdom, Ireland	Switchvox Cloud, Switchvox as a Service, PBXact Cloud
Salesforce	Storage of customer contact details	Phones numbers, addresses, service quotes	USA	Switchvox Cloud, Switchvox as a Service, SIPStation, PBXact Cloud
Sangoma Affiliates	Service support, management functions, maintenance and operation of the Services	All data provided and collected related to the Services.	USA, United Kingdom, Ireland, Australia, India, Philippines, Ecuador, Columbia	Switchvox Cloud, Switchvox as a Service, SIPStation, PBXact Cloud