DATA PROCESSING AGREEMENT

Effective Date: October 3rd, 2025	
("Subscriber")	**IcePanel Technologies Inc.** **("IcePanel")**
Signature:	Signature:
The Parties consent to execution of this DPA by one or both Parties using electronic signatures.	
Name:	Name:
Title:	Title:
Signature Date:	Signature Date:
Notice Address:	Notice Address: 1500 West Georgia, Suite 1300 Vancouver, British Columbia V6G 2Z6, Canada

1. IcePanel has entered into one or more Agreements with Subscriber to provide Services involving Processing of Personal Data. This Data Processing Agreement ("**DPA**") is effective as of the Effective Date by and between IcePanel and Subscriber. This DPA shall apply to all Processing of Personal Data that Subscriber, Subscriber Affiliates or Subscriber Agents provide or make accessible to IcePanel in connection with IcePanel's performance of all Services under the Agreement, and is incorporated into the Agreement by reference. Capitalized terms used in this DPA shall have the meaning set forth below unless otherwise defined in this DPA:

    a. "**Affiliate**" means any person or entity that, either directly or indirectly, owns, controls, is controlled by, or is under common control with a Party, where control is defined as owning or directing more than fifty percent (50%) of the voting equity securities or a similar ownership interest in the controlled entity;

    b. "**Agent**" means any third party (including subcontractors, independent contractors, customers or authorized users as applicable) that may provide Services on behalf of IcePanel, or to whom Services are provided or made accessible on behalf of Subscriber, in connection with performance of the Agreement;

    c. "**Agreement**" means all current and future agreements between IcePanel and Subscriber in connection with which IcePanel provides Services involving the Processing of Personal Data on behalf of Subscriber. This DPA is incorporated into such Agreements by this reference;

    d. "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU Data Protection Laws and the California Data Protection Law;

    e. "**Authorized Persons**" means any IcePanel Agents, Sub-Processors or IcePanel personnel who Processes Personal Data on IcePanel's behalf;

f. "**Subscriber**" means the Subscriber Party entering into this DPA with IcePanel and/or the Subscriber Affiliate(s) on whose behalf or at whose direction IcePanel Processes Personal Data;

g. "**California Data Protection Law**" means the CCPA until December 31, 2022 and the CPRA as of January 1, 2023;

h. "**CCPA**" means the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq., and its implementing regulations as in effect until December 31, 2022; as of January 1, 2023, any reference to the CCPA shall be construed as a reference to the CPRA;

i. "**CPRA**" means the California Privacy Rights Act Cal. Civ. Code section 1798.100 et seq., and its implementing regulations, as in effect from January 1, 2023; before January 1, 2023, any reference to the CPRA shall be construed as a reference to the CCPA;

j. "**IcePanel**" means the entity (-ies) entering into the DPA with Subscriber;

k. "**EU Data Protection Laws**" means the EU General Data Protection Regulation (Regulation 2016/679) and any other applicable EU or Member State laws and regulations that apply to the Processing of Personal Data; by extension, "**EU Data Protection Laws**" also encompass the United Kingdom's Data Protection Act 2018 to the extent that it is applicable to the Personal Data;

l. "**Services**" means any cloud offering, professional, consulting, advisory, development or all other services performed by IcePanel for Subscriber;

m. "**Sub-Processor**" means any IcePanel Agent and/or IcePanel Affiliate(s) engaged directly by or indirectly on behalf of IcePanel to Process any Personal Data relating to this Agreement and/or the Services;

n. "**Controller**", "**Processor**", "**Data Subject**", "**Processing**" (and "**Process**") shall have the meanings given in Applicable Data Protection Law. If and to the extent that Applicable Data Protection Laws do not define such terms, then the definitions given in EU Data Protection Laws will apply;

o. "**Personal Data**" and **Personal Information** means personal information as defined in Applicable Data Protection Law (or, if Applicable Data Protection Laws do not define such terms, as defined in EU Data Protection Laws) as processed by IcePanel on behalf of Subscriber under the terms of this Agreement;

p. **"UK IDTA"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, which has been issued by the United Kingdom's Information Commissioner for Parties making Restricted Transfers and incorporated as Annex 2B to this DPA;

q. "**Model Clauses**" means the agreement pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 (Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council) as officially published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN;

r. "**Legal Process**" means any request to disclose Subscriber Personal Data made under law from a public authority, including judicial authorities, including but not limited to court orders, subpoenas, warrants or similar process.

2. **Role and Scope of Processing**: Subscriber appoints IcePanel to Process Personal Data in connection with the scope set out in Annex 1 to this DPA as a Processor acting on behalf of Subscriber as Controller. IcePanel shall comply with the obligations that apply to it under Applicable Data Protection Law, the Agreement and this DPA.

3. **Purpose Limitation**: IcePanel will at all times, and will ensure any Authorized Persons, Process Personal Data only as necessary for the purposes of: (i) providing the Services to Subscriber; (ii) performing its obligations under this Agreement; and (iii) strictly

in accordance with Subscriber's documented instructions ("**Permitted Purpose**"). In no event shall IcePanel Process Personal Data for any of its own purposes or those of any third party.

4. **Sub-Processing**: IcePanel shall not subcontract any Processing of the Personal Data without the consent of Subscriber. Subscriber consents to IcePanel engaging Sub-Processors to Process the Personal Data provided that: (i) IcePanel provides Subscriber at least thirty (30) days' prior written notice of addition or removal of any Sub-Processor (including details of proposed Processing); (ii) IcePanel engages Sub-Processors through a written agreement including data protection terms at least as protective as the Agreement (including this DPA); and (iii) IcePanel remains fully liable and responsible for the performance of the Agreement (including this DPA) and for the acts, non-acts, errors or omissions of its Sub-Processors.

5. **California Privacy Rights.**

   (a) Subscriber is the Business and IcePanel is the Service Provider, for purposes of California Data Protection Law.

   (b) Subscriber discloses Personal Information to IcePanel solely for the purpose of IcePanel's provision of the Services contemplated under the Agreement, exclusively for Subscriber's business purposes specified therein.

   (c) Subscriber is entitled to: (i) take reasonable and appropriate steps to ensure that IcePanel uses Personal Information in a manner consistent with Subscriber's obligations under California Data Protection Law, provided that the foregoing shall not interfere or place an undue burden on IcePanel's systems; (ii) monitor IcePanel's compliance through measures, including ongoing manual reviews, and regular assessments not more than once every 12 months; and (iii) take, upon notice, reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information by IcePanel, including but not limited to terminating the Agreement.

   (d) IcePanel shall: (i) not sell or share Personal Information; (ii) not retain, use, or disclose the Personal Information: (A) outside the direct business relationship between IcePanel and Subscriber; or (B) for any purpose other than for the business purposes specified in the Agreement, unless otherwise permitted by the California Data Protection Law; (iii) upon instruction by Subscriber, stop using Sensitive Personal Information for any purpose other than providing the Services to the extent IcePanel has actual knowledge that the Personal Information is Sensitive Personal Information; (iv) not combine Subscriber Personal Information with other Personal Information that IcePanel receives from, or on behalf of, another person or collects from its own interaction with consumers, unless permitted by California Data Protection Law; (v) refrain from attempting to re-identify any de-identified information disclosed by Subscriber to IcePanel under the Agreement; (vi) only subcontract any Processing of Personal Information pursuant to Section 4 of this DPA ("Sub-Processing"), and, to the extent commercially feasible, enable Subscriber to be promptly notified if IcePanel's Sub-Processor further subcontracts any Processing of Personal Information; (viii) assist Subscriber in responding to verifiable consumer requests pursuant to Section 11 of this DPA ("Cooperation and Data Subjects' rights"); (ix) refrain from complying with consumer deletion request submitted directly to IcePanel to the extent that IcePanel has collected, used, processed, or retained the Personal Information in its role as Service Provider to Subscriber; (x) promptly notify Subscriber if IcePanel determines that it can no longer meet its obligations under California Data Protection Law or under this Section; and (xi) remain liable for IcePanel's own violations of California Data Protection Law. "Business," "**Personal Information,**" "**Selling,**" "**Sensitive Personal Information,**" "Services" and "Service Provider" as used in this Section shall have the meaning set forth in California Data Protection Law.

6. **Security**: IcePanel shall comply with the minimum information security controls defined in the Agreement as applicable to Services involving the Processing of Personal Data (the "**Controls**"), and shall implement further appropriate technical, physical, and organizational measures and safeguards for protection of the security, confidentiality and integrity of the Personal Data and to protect the Personal Data from the following, (each and every, a "**Security Incident**"): (i) accidental or unlawful destruction, and/or (ii) unauthorized loss, alteration, acquisition, use, disclosure or access by a third party.

7. **Supplementary Measures**: For Personal Data collected in the European Economic Area ("EEA"), IcePanel shall collaborate with Subscriber in the event of international data transfer from the EEA to a country not recognized by the European Commission as offering an adequate level of data protection in the meaning of GDPR Article 45. For the appropriate safeguards contained in the Article 46 GDPR transfer tools to be effective, IcePanel shall comply with the following supplementary measures: (i) provide encryption key management pursuant to the Controls; (ii) to the extent legally permissible, (a) provide prompt written notice to Subscriber of any Legal Process; such notice shall include information about Personal Data requested, requesting authority, the legal basis for the Legal Process and IcePanel's response provided; (b) use commercially reasonable efforts, and provide reasonable assistance to Subscriber, to object to or limit any Legal Process that Subscriber or IcePanel reasonably determines is overbroad, incompatible with applicable law or otherwise unlawful; and (c) disclose the minimum amount of Personal Data as reasonably necessary to comply with Legal Process; and (iii) Section 15 of this DPA, Destruction or Return of Personal Data.

8. **Confidentiality of Processing**: IcePanel and its Authorized Persons shall: (i) Process the Personal Data only as necessary for the Permitted Purpose; and (ii) limit access to Personal Data only to those Authorized Persons: (a) who need to have access in order to perform the Services; (b) are trained in the care and handling of Personal Data; and (c) are subject to a strict duty of confidentiality (whether a contractual or statutory duty) with respect to the Personal Data they Process.

9. **Cooperation**: Where IcePanel will host Personal Data or undertake any business Process function on Subscriber's behalf, IcePanel shall cooperate with Subscriber in taking reasonable steps to ensure that the Personal Data is accurate, complete and current, including, without limitation, amending records when it becomes aware that such Personal Data in its possession is inaccurate or incomplete.

10. **Data Protection and Data Transfer Impact Assessments**: Upon Subscriber's request or, if IcePanel believes or becomes aware that its Processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, IcePanel shall promptly inform Subscriber in writing where applicable and provide Subscriber with all such reasonable and timely assistance as Subscriber may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority. Upon Subscriber's request, IcePanel shall promptly provide such information and assistance as needed to assess the impact of data transfers performed by IcePanel pursuant to section 12 of this DPA.

11. **Cooperation and Data Subjects' rights**: IcePanel shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Subscriber to enable Subscriber to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any correspondence, enquiry or complaint received from a Data Subject, regulator, data protection authority or third party in connection with the Processing of the Personal Data. IcePanel shall promptly provide to Subscriber any such request, correspondence, enquiry or complaint made indirectly or directly to IcePanel.

12. (a) International Transfers: IcePanel will at all times provide an adequate level of protection for the Personal Data wherever Processed, in accordance with the requirements of Applicable Data Protection Law. IcePanel shall not Process or transfer any Personal Data processed by IcePanel on behalf of Subscriber outside of the EEA unless it: takes all such measures as are necessary to ensure such Processing or transfer is in compliance with Applicable Data Protection Laws and/or any such measures as are provided for in this Agreement. For Personal Data subject to EU Data Protection Laws and/or that originates from the EEA and Switzerland ("**EU Data**") and/or from the United Kingdom ("**UK Data**"), such measures may include transferring (directly or via onward transfer) the EU Data and/or UK Data to: (i) a recipient in a country that the European Commission, the Swiss Federal Data Protection Authority or the United Kingdom Data Protection Authority (as applicable) has decided provides adequate protection for EU Data or UK Data (as applicable); and/or (ii) a recipient that has executed the Model Clauses (and UK IDTA as applicable).

(b) Model Clauses and UK IDTA: Transfers of EU Data rely on the Model Clauses incorporated as Annex 2A to the DPA, and transfers of UK Data rely on the Model Clauses and UK IDTA incorporated as Annexes 2A and 2B respectively to this DPA, with Subscriber as data exporter and IcePanel as data importer. IcePanel shall at all times comply with (and ensure that all

Sub-Processors comply with) the Model Clauses and UK IDTA as applicable. To the extent the Model Clauses or UK IDTA conflict with any provision(s) of this DPA, the Model Clauses or UK IDTA shall prevail, to the extent of that conflict or inconsistency.

(c) Notice of Non-Compliance: If IcePanel determines or believes that it and/or its Sub-Processors can no longer meet its obligations under this Section (including Applicable Data Protection Law), IcePanel shall: (i) immediately notify Subscriber in writing and work with Subscriber (including by following the lawful written instructions of Subscriber) and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any Processing (including transfer) until such time as the Processing (including transfer) meets the level of protection as is required by this Section; and (ii) immediately stop (and ensure that all Sub-Processors immediately stop) Processing all Personal Data, if in Subscriber's sole discretion, Subscriber determines or believes that IcePanel and/or its Sub-Processors have not or cannot correct any non-compliance with this Section, as described herein within a reasonable time frame determined by Subscriber.

13. Security Incidents: IcePanel shall notify Subscriber without undue delay (and, in any event, within 72 hours) upon becoming aware of a Security Incident and shall provide all such timely information and cooperation as Subscriber may require in order for Subscriber to fulfil its data breach reporting obligations under (and in accordance with timeline required by) Applicable Data Protection Law. IcePanel shall further take all such measures and actions as are necessary to promptly remedy or mitigate the effects of the Security Incident and shall keep Subscriber updated on all developments in connection with the Security Incident. IcePanel shall notify Subscriber immediately in writing upon becoming aware of: (i) any breach of this DPA or of any Applicable Data Protection Law; and/or (ii) any inquiry, investigation or enforcement proceeding relating to IcePanel's data privacy compliance generally or the Agreement (including this DPA). IcePanel shall defend, indemnify and hold Subscriber harmless from and against any loss, damage, liabilities, fees, or costs (including reasonable attorneys' fees and other legal expenses) in connection with any claims, demands, suits, or proceedings, including fines or penalties issued by a data protection authority, made or brought against Subscriber by a third party arising out of or in connection with a breach of this DPA or of any Applicable Data Protection Law and such indemnification obligation shall not be subject to any limits to IcePanel's liability under the Agreement.

14. **Audit**: (a) Upon reasonable prior written notice from Subscriber and not more than once per year (unless arising from exigent circumstances, such as confirmed Security Incident or permissible under applicable law), and subject to the parties' confidentiality obligations, IcePanel will make available for Subscriber review records containing all information necessary to demonstrate IcePanel's compliance with IcePanel's obligations under the DPA and Applicable Data Protection Law. IcePanel will provide, Subscriber physical access to its facilities as may be reasonably requested to verify IcePanel's compliance with its obligations under the DPA and Applicable Data Protection Law, if (a) IcePanel does not provide sufficient records demonstrating its compliance with the information security controls defined in the Agreement; (b) a confirmed Security Incident has occurred; (c) a written request for physical inspection is made by Subscriber's or its end user's Supervisory Authority; or (d) Applicable Data Protection Law provides Subscriber or its end user with a mandatory physical inspection right.

    (b) Any audit or inspection will be conducted during IcePanel's regular business hours, in a manner that does not unreasonably interfere with operations. Any audit may be conducted by Subscriber personnel or third party expert selected by Subscriber that is not a IcePanel competitor.

    (c) Where IcePanel acts as Processor on behalf of Subscriber's end users, IcePanel shall provide the same audit records and access directly to Subscriber's end user, subject to confidentiality obligations between Subscriber and its end user.

15. Destruction or Return of Personal Data: No later than ninety (90) days from termination or expiry of the Agreement or earlier upon Subscriber's request, IcePanel shall, and shall cause its Sub-Processors to return to Subscriber or destroy and certify destruction of Personal Data. This requirement shall not apply: (i) to the extent that IcePanel is required by Applicable Data Protection Law to retain Personal Data; and/or (ii) Personal Data stored on IcePanel's or Sub-Processor's automatic electronic backup or disaster recovery systems until deleted in the ordinary course thereof; provided that IcePanel refrains from further

Processing the Personal Data in performance of the Agreement, and complies with the DPA until Personal Data is returned or destroyed.

16. **General**: Applicable law, venue and jurisdiction for this DPA are those of the Agreement. If there is any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict or inconsistency. Notwithstanding anything else to the contrary in the Agreement, the obligations placed upon the IcePanel under this DPA shall survive so long as IcePanel and/or its Sub-Processors Processes Personal Data on behalf of Subscriber. If an amendment to this DPA is required to comply with applicable law or Subscriber's reasonable requirements for the protection of Personal Data, the Parties will work together in good faith to promptly agree upon and execute such amendment. Where IcePanel rejects Subscriber's reasonable requested changes, Subscriber may terminate without liability (except for the payment of fees for Services rendered) all or part of the Agreements and this DPA with thirty (30) days' written notice.

ANNEX 1 TO DPA: PROCESSING SCOPE

PROCESSING SCOPE:

Subject Matter:

The objective of Processing of Personal Data by IcePanel is the performance of the Services pursuant to the standard Terms of Service or Master Agreement.

Duration:

IcePanel will Process Personal Data continuously for the duration of the standard Terms of Service or Master Agreement and will delete all Personal Data following termination in accordance with section 8(C), unless otherwise agreed upon in writing.

Nature and Purpose of Processing:

The objective of Processing of Personal Data by IcePanel is the performance of the Services pursuant to the standard Terms of Service or Master Agreement.

Types of Personal Data:

Customer may submit Personal Data to the services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Identifier
- Name
- Work email
- Job role
- Country
- City
- Region
- Machine info
- Browser info
- IP address
- Business address
- Business tax identifier
- Business phone number
- Card information

Categories of Data Subject:

Prospective customers, customers and users *who use the Service (who are natural persons) ("User")"*

The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):

Categories of individuals	**Categories of personal data**	**Purpose of processing**
Prospective customers	Identifier, name, work email, job role, business phone number	Relationship management, customer communication
Customers	Identifier, name, work email, job role, country, city, region, machine info, browser info, IP address, business address, business tax identifier, business phone number, card information, signatures	App functionality, customer support, user analytics, data storage, backup storage, error tracking, security threat detection, subscription management, transactional communication, invoices, receipts, financial reporting, payment processing, legal contracts, marketing communication, request tracking, relationship management
Users	Identifier, name, work email, job role, country, city, region, machine info, browser info, IP address	App functionality, customer support, user analytics, data storage, backup storage, error tracking, security threat detection, subscription management, transactional communication, marketing communication, request tracking

Sub-Processors:

IcePanel shall keep an up-to-date list of all Sub-Processors in this Addendum. When subscribed to notifications at https://trust.icepanel.io/updates, IcePanel shall notify Subscriber, at least 30 days in advance in writing, in the event that IcePanel proposes to add any additional Subprocessors. Subscriber has the right to raise objections to any changes within the 30 day notification period.

IcePanel uses the following Sub-Processors:

Name of subprocessor	**Purpose of processing**	**Categories of personal data**	**Third countries personal data is transferred to**	**Retention schedule**
Algolia, Inc	Search functionality, data storage	Identifier, name, work email	United States	End of customer relationship or

				12 months for backups
Attio	Customer relationship manager	Identifier, name, work email, company, job role, country, city, region	United Kingdom	End of customer relationship
Cal.com, Inc	Calendar scheduling	Name, work email, job role	United States	Indefinitely
Canny, Inc	Customer feedback and requests	Name, work email	United States	Indefinitely
Customer.io	Outbound marketing	Identifier, name, work email, company, job role, country, city, region	United States	End of customer relationship
Datadog, Inc	Security thread detection	Identifier, name, work email, job role, country, city, region, machine info, browser info, IP address	United States	15 months
DocuSign, Inc	Invoices, legal contracts	Name, work email, job role, business address, business tax identifier, business phone number, signatures	United States	Indefinitely
Google Cloud (Google LLC)	App functionality, customer support, user analytics, data storage, backup storage	Identifier, name, work email, job role, IP address	United States	End of customer relationship or 12 months for backups
Google Workspace (Google LLC)	Invoices, receipts, customer support, legal contracts, user analytics	Name, email, job, role, country, city, business address, business tax identifier, business phone number, signatures	United States	End of customer relationship or indefinitely for invoices, receipts, legal contracts

Linear Orbit	Request tracking, customer support	Identifier, name, work email	United States	End of customer relationship
Missive (Heliom, Inc)	Customer support	Identifier, name, work email, job role	United States	End of customer relationship
Mixpanel, Inc	User analytics, customer support	Identifier, name, work email, job role, country, city, region	United States	End of customer relationship
OpenAI	Data processing and enriching	Identifier, name, work email	United States	End of customer relationship
Posthog, Inc	User analytics, customer support	Identifier, name, work email, job role, country, city, region	United States	End of customer relationship
Notion Labs, Inc	Customer feedback, pilot tracking	Identifier, name, work email, job role	United States	End of customer relationship
Resend (Plus Five Five, Inc)	Transactional and marketing communication	Identifier, name, work email, job role	United States	End of customer relationship
Sentry (Functional Software, Inc)	Error tracking, customer support	Identifier, name, work email, job role, machine info, browser info, IP address	United States	End of customer relationship
Slack Technologies, LLC	Customer support, user analytics	Identifier, name, work email, job role, machine info, browser info	United States	End of customer relationship
Stripe, Inc	Payment processing, subscription management, invoices, receipts, financial reporting	Identifier, name, work email, business address, business tax identifier, business phone number, card information	United States	End of customer relationship or indefinitely for invoices, receipts
Xero Limited	Invoices, receipts, financial reporting	Name, work email, job role, business address, business tax identifier, business phone number	United States	Indefinitely

ANNEX 2A TO DPA: MODEL CLAUSES
(FOR EU/EEA AND SWISS DATA EXPORTERS, MODULE 2)

SECTION I

Clause 1 – Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 – Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 – Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8, Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9, Clause 9(a), (c), (d) and (e);
(iv) Clause 12, Clause 12(a), (d) and (f);
(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18, Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 – Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 – Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 – Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of

processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(d) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(e) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(f) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 – Use of Sub-Processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of Sub-Processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the Sub-Processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a Sub-Processor to carry out specific Processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the Sub-Processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a Sub-Processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the Sub-Processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the Sub-Processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the Sub-Processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the Sub-Processor contract and to instruct the Sub-Processor to erase or return the Personal Data.

Clause 10 – Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the Processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 – Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 – Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its Sub-Processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its Sub-Processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a Processor acting on behalf of a Controller, to the liability of the Controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its Sub-Processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a Sub-Processor to avoid its own liability.

Clause 13 – Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 – Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the Processing of the Personal Data by the data importer, including any requirements

to disclose Personal Data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the Processing of the Personal Data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 – Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 – Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of Personal Data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:

(i) The data exporter has suspended the transfer of Personal Data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal Data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred Personal Data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of Personal Data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the Processing in question under Regulation (EU) 2016/679.

Clause 17 – Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18 – Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX A TO MODEL CLAUSES

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name:

Address:

Contact person's name, position and contact details (written out in full):

Activities relevant to the data transferred under these Clauses: Data Processing services ordered from the data importer(s) per the Agreement

Signature and date:

Role (Controller/Processor): **Controller**

2. All Subscriber Affiliates as defined in the Agreement

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name:

IcePanel Technologies Inc.

Address:

1500 West Georgia, Suite 1300

Vancouver, British Columbia

V6G 2Z6, Canada

Contact person's name, position and contact details (written out in full):

Activities relevant to the data transferred under these Clauses: Provision of the Sub-Processing services ordered from the data exporters per the Agreement

Signature and date:

Role (Controller/Processor): **Processor**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred

As specified in the Agreement

Categories of Personal Data transferred

As specified in the Agreement

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.

As specified in the Agreement

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

As specified in the Agreement

Nature of the Processing

As specified in the Agreement

Purpose(s) of the data transfer and further Processing

As specified in the Agreement

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

As specified in the Agreement

For transfers to (Sub-) Processors, also specify subject matter, nature and duration of the Processing

As specified in the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

- For matters related to data transfers pursuant to Regulation (EU) 2016/679:

Autoriteit Persoongegevens of the Netherlands: https://www.autoriteitpersoonsgegevens.nl/en

- For matters related to data transfers pursuant to, until December 31, 2022, the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; "FADP"), and from January 1, 2023 onwards, the Revised Swiss Federal Act on Data Protection of 25 September 2020 ("Revised FADP"):

Federal Data Protection and Information Commissioner of Switzerland: https://www.edoeb.admin.ch/edoeb/en/home.html

APPENDIX B TO MODEL CLAUSES: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

As described in the applicable Controls in the Agreement(s).

For transfers to (Sub-) Processors, also describe the specific technical and organisational measures to be taken by the (Sub-) Processor to be able to provide assistance to the Controller and, for transfers from a Processor to a Sub-Processor, to the data exporter.

The data importer(s) shall contractually require all of their Sub-Processors to take technical and organisational measures at least equivalent to, and in any case no less protective than those referenced above.

APPENDIX C TO MODEL CLAUSES: THIRD-COUNTRY ADDENDUM FOR SWITZERLAND

For the purposes of these Clauses, the term 'member state' shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

Until December 31, 2022, these Clauses shall also protect the data of legal entities in the scope of the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; "FADP").

ANNEX 2B TO DPA: International Data Transfer Addendum (FOR UK DATA EXPORTERS) - UK IDTA

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	November 27, 2024	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address: Official registration number (if any): **See details for Data Exporter in Appendix A to Model Clauses**	Full legal name: **IcePanel Technologies Inc.** Trading name (if different): Main address (if a IcePanel registered address): 1500 West Georgia, Suite 1300 Vancouver, British Columbia V6G 2Z6, Canada Official registration number: BC1344197 **See details for Data Importer in Appendix A to Model Clauses**
Key Contact	Full Name (optional):	Full Name: Victor Leach Job Title: Director

	Job Title: Contact details including email: **See contact details for Data Exporter in Appendix A to Model Clauses**	Contact details including email: victor@icepanel.io **See contact details for Data Importer in Appendix A to Model Clauses**
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date of the DPA Reference (if any): See Model Clauses Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	N/A	N/A			

2	Yes	Yes	No	General	30 days	
3	No	N/A	N/A	N/A	N/A	
4	No	N/A	N/A			N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Appendix A to Model Clauses
Annex 1B: Description of Transfer: See Annex 1 to DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Appendix B to Model Clauses
Annex III: List of Subprocessors (Modules 2 and 3 only): See Appendix A to Model Clauses

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.