DATA PROCESSING ADDENDUM

This Data Processing Addendum, ("**DPA**") made between Modular Mining Systems Inc. and other Komatsu affiliates and subsidiaries ("**Komatsu**") and the customer whose name appears on the relevant order form or contract, including all of customer's Affiliates (**"Customer"**) (together, the "**Parties**"), forms part of the Agreement between Komatsu and Customer ("**Agreement**") and reflects the Parties' agreement regarding the Processing of Customer Personal Data.

1. Definitions

1.1 The terms "**Controller,**" "**Data Subject,**" "**Personal Data,**" "**Personal Data Breach,**" "**Processing,**" "**Processor,**" "**Sell**," "**Share**," "**Supervisory Authority,**" and analogous or cognate terms shall have the meaning provided under applicable Data Protection Laws (or, where not defined in applicable Data Protection Law, shall have the meaning as in the GDPR).

1.2 In this DPA, capitalized terms that are not defined herein shall have the meanings set out in the Agreement. The following terms shall have the meanings set out below (and cognate terms shall be construed accordingly):

1.2.1 "**Customer Personal Data**" means any Personal Data that is Processed by Komatsu on behalf of Customer pursuant to, or in connection with, the Agreement and this DPA; as between the Parties, all Customer Personal Data shall be, and shall remain the property of, Customer or its respective clients;

1.2.2 "**Affiliate**" means an entity that owns or controls, is owned or controlled by, or is or under common control or ownership of Customer or Komatsu, where control is defined as the possession, directly or indirectly, of the power to direct, or cause the direction of, the management and policies of an entity;

1.2.3 **"Agreement"** has the meaning set out in the preamble;

1.2.4 **"CCPA"** means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020;

1.2.5 **"CRM Data"** means business contact information such as names, email addresses, title, and telephone numbers for Customer employees, contractors, agents and representatives, and other data and information (including any Personal Data) that Komatsu (on its own behalf as a Controller) collects and processes as necessary to the management of Komatsu's business relationship with Customer;

1.2.6 "**Data Protection Law(s)**" means all international, national, federal, state, provincial, or local privacy, cybersecurity, and data protection laws, including, without limitation, the CCPA, the GDPR, Brazil's Data Protection Law No. 13,709/2018, Canada's Personal Information Protection and Electronic Documents Act, the Act Respecting the Protection of Personal Information in the Private Sector (Quebec), the Personal Information Protection Act (Alberta), the Personal Information Protection Act (British Columbia), Australia's Privacy Act 1988 (Cth), India's Digital Personal Data Protection Act, and South Africa's Protection of Personal Information Act, together with any implementing or supplemental rules and regulations, applicable to the processing of Personal Data under this DPA, as amended or replaced from time to time;

1.2.7 **"GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and associated national legislation;

1.2.8 "**Member State**" means a member state of the European Economic Area ("**EEA**");

1.2.9 "**Restricted Transfer**" means a transfer or an onward transfer of Customer Personal Data where such transfer would be prohibited or restricted by Data Protection Law in the absence of an adequacy decision, a permitted derogation, or protection for the transferred Customer Personal Data provided by binding corporate rules, SCCs, or other mechanism specified under applicable Data Protection Law. For clarity, a transfer of Customer Personal Data originating from the province of Quebec, Canada, to another jurisdiction (including to other Canadian provinces) shall constitute a Restricted Transfer to the extent required under applicable Data Protection Law;

1.2.10 "**SCCs**" means, as applicable to the relevant data transfer: (i) **Module 2** (Controller to Processor, applicable when Customer is the Controller of Customer Personal Data), or **Module 3** (Processor to Processor, applicable when Customer is processing Customer Personal Data on behalf of its clients) of the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 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 ("**EU SCCs**"), (ii) the UK IDTA, or (iii) such other terms intended to provide adequate protection to transferred Personal Data pursuant to Data Protection Law; in each case, as amended or replaced from time to time under the relevant Data Protection Law;

1.2.11 **"Security Incident"** means (i) any Personal Data Breach affecting Customer Personal Data, or (ii) any other event resulting in the unauthorized or unlawful access to, use, disclosure, loss, alteration or destruction of Customer Personal Data. Security Incident will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems;

1.2.12 **"Sensitive Personal Data"** has the meaning provided under applicable Data Protection Law, and includes its cognate terms. For avoidance of doubt, Sensitive Personal Data shall include any Personal Data subject to heightened restrictions or regulations, including "protected health information," "consumer health data," and "nonpublic personal information."

1.2.13 **"Services"** means the services provided by Komatsu pursuant to, or in furtherance of, the Agreement;

1.2.14 "**Subprocessor**" means any Processor (including any third party and any Komatsu Affiliate, but excluding an employee of Komatsu or an employee of any of its sub-contractors) appointed by, or on behalf of, Komatsu to Process Customer Personal Data;

1.2.15 **"Third Country"** means: (i) with respect to GDPR, a country other than the Member States; (ii) with respect to the UK Data Protection Law, any country outside of the UK; and (iii) with respect to any other country, as provided in relevant Data Protection Law;

1.2.16 "**UK Data Protection Law**" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 ("**UK GDPR**"), together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), and other Data Protection Laws in force from time to time in the United Kingdom; and

1.2.17 "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

2. Processor Obligations

2.1 Customer is either a Controller or a Processor of Customer Personal Data, and Komatsu is a Processor with respect to all Customer Personal Data, and a Controller with respect to CRM Data. Where applicable Data Protection Law uses terms other than Controller and Processor, the appropriate terms shall be understood to apply as the context requires.

2.2 Details of the Processing are set out in **Annex 1** to this DPA.

1.1 Customer instructs Komatsu (and authorizes Komatsu to instruct each Subprocessor) to Process Customer Personal Data, including transferring Customer Personal Data to a Third Country, subject always to Komatsu complying with the terms of this DPA, as reasonably necessary to provide the Services.

2.3 Komatsu shall at all times comply with applicable obligations under Data Protection Law, and shall:

2.3.1 process Customer Personal Data only for the specific purposes of the Processing as set out in **Annex 1** or as otherwise instructed by Customer, unless Processing is required by Data Protection Law to which Komatsu is subject, in which case Komatsu shall inform Customer of that legal requirement before such Processing, unless that law prohibits such information on important grounds of public interest;

2.3.2 promptly revert to Customer to seek clarification if the instructions issued by Customer are unclear, and inform Customer if, in Komatsu's opinion, such instructions infringe Data Protection Law;

2.3.3 grant access to Customer Personal Data only to the extent necessary for performing the Services, and ensure that all persons authorized to process Customer Personal Data are appropriately trained, and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.3.4 implement the technical and organizational measures specified in **Annex 2** to ensure the security of Customer Personal Data, taking due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for Data Subjects; and, further, if, at any

time, an authority mandates specific additional measures, the Parties shall work together in good faith to implement such measures;

2.3.5 where Komatsu is obligated by Data Protection Law to maintain a record of Processing activities, Komatsu shall maintain a record of its Processing activities conducted for and on behalf of Customer in accordance with Data Protection Law.

2.4 Nothing in this DPA shall prevent Komatsu from Processing Komatsu CRM Data for its own purposes in its capacity as a Controller, provided that such Processing is reasonably necessary for Komatsu's management of its business relationship with Customer and is in compliance with applicable Data Protection Law.

3. **Customer Obligations**

3.1 Customer shall, including on behalf of any Controller for whom it acts as a Processor and on behalf of its Affiliates who may use the Services, serve as a single point of contact for Komatsu in all matters under this DPA and shall be responsible for the internal coordination, review and submission of instructions or requests to Komatsu as well as the onward distribution of any information, notifications, or reports provided by Komatsu hereunder.

3.2 Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer represents that, where required by applicable Data Protection Law, it has obtained all necessary consents from and provided all necessary notices to Data Subjects for its collection and Processing of Customer Personal Data. Customer represents that its use of the Services will not violate the rights of any individual that has opted-out from the Sale or Sharing of, or other disclosure of, Customer Personal Data, to the extent applicable under Data Protection Law.

3.3 Customer agrees that Komatsu shall not be liable for any breach of applicable Data Protection Law to the extent Komatsu has processed Customer Personal Data in accordance with the instructions from Customer, and Customer shall be solely liable for any such breach and shall indemnify Komatsu for any fines, costs, or damages relating to same, provided that Komatsu will promptly inform Customer if, in its opinion, any instruction or request entails any non-compliance with applicable Data Protection Law. The Parties acknowledge that Komatsu is not obligated to undertake additional work or analysis beyond the scope of the Services to determine if Customer's instructions are compliant with applicable Data Protection Law.

3.4 Customer shall not provide, disclose, or otherwise make available to Komatsu any Sensitive Personal Data without providing Komatsu prior written notice and obtaining Komatsu's express written consent. In the event that Customer intends to provide Sensitive Personal Data, the Parties shall cooperate to implement any additional technical, organizational, or contractual measures reasonably required to ensure compliance with applicable Data Protection Law and to mitigate any associated risks. Komatsu reserves the right to refuse to process any Sensitive Personal Data at its sole discretion. Customer shall remain solely responsible and liable for any Sensitive Personal Data provided to Komatsu in breach of this provision and shall indemnify and hold harmless Komatsu from and against any and all claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to such provision or processing of Sensitive Personal Data.

4. **CCPA Terms.**

4.1 To the extent that Komatsu Processes any Customer Personal Data subject to the CCPA, Komatsu agrees to the following with respect to such Personal Data only:

4.1.1 All Customer Personal Data disclosed by Customer to Komatsu, or that Komatsu receives or processes on Customer's behalf, is disclosed or received only for limited and specified purposes, including for one or more business or commercial purposes as those terms are defined under the CCPA.

4.1.2 Komatsu shall not Sell, Share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Customer Personal Data received from, or on behalf of, Customer to any third party for monetary or other valuable consideration.

4.1.3 Komatsu shall not retain, use, or disclose Customer Personal Data received from, or on behalf of, Customer: (i) for any purposes other than a business purposes specified in the Agreement, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Komatsu.

4.1.4 Komatsu may combine Personal Data that it receives from, or on behalf of, Customer with Personal Data that Komatsu receives from, or on behalf of, another person, or collects from its own interaction with an individual, unless the combining of that Personal Data is prohibited by the CCPA. For purposes of this DPA, "combine" means to aggregate Personal Data about an individual into a single profile.

4.1.5 If Customer provides Komatsu with deidentified Personal Data, or if Komatsu deidentifies Personal Data previously provided by Customer, Komatsu agrees to take reasonable measures to ensure that the

deidentified Personal Data cannot be associated with a consumer or household, and not attempt to reidentify the Personal Data.

4.1.6 If Komatsu makes a determination it can no longer meet its obligations under the CCPA, it shall promptly notify Customer of this fact.

4.1.7 Komatsu certifies it understands the obligations and restrictions above and will comply with them.

5. Subprocessing

5.1 Komatsu's current list of Subprocessors engaged in Processing of Personal Data on behalf of Komatsu (Subprocessor List) can be found in Annex 3 of this Agreement. Customer hereby grants Komatsu general written authorization to retain the Subprocessors found on the Subprocessor List. Komatsu will provide 30 days' notice prior to engaging a new Subprocessor. Should Customer reasonably object to the addition of a Subprocessor by Komatsu within the 30-day window, the Parties shall negotiate in good faith to find a suitable alternative Subprocessor. If no agreement is reached between the Parties, Customer shall have the right to terminate the Agreement as it relates to the use of the objected-to Subprocessor by Komatsu. Customer hereby consents to the Subprocessors listed in **Annex 3** hereto, subject to the conditions set out in Section 5.2.

5.2 With respect to each Subprocessor, Komatsu shall:

5.2.1 enter into a written agreement with the Subprocessor imposing terms that are consistent with those set out in this DPA or otherwise sufficient to meet the requirements of applicable Data Protection Laws;

5.2.2 remain liable to Customer for any act or omission of its Subprocessor;

5.2.3 upon Customer request, provide Customer with a summary of the Processing to be undertaken by each Subprocessor; and

5.2.4 if the arrangement involves a Restricted Transfer, ensure that the relevant SCCs or transfer mechanism is, at all relevant times, entered into between Komatsu and the Subprocessor.

5.3 Where Komatsu engages a Komatsu Affiliate as a Subprocessor, such Komatsu Affiliate may engage further Subprocessors subject to all the above terms and conditions.

6. Security Incident

6.1 Komatsu shall notify Customer without undue delay, but after a reasonable period to allow Komatsu to investigate and, if necessary, involve law enforcement, upon Komatsu becoming aware of an actual Security Incident. Komatsu shall provide Customer with sufficient information to allow Customer to meet its obligations to assess and report a Security Incident under applicable Data Protection Law, which may be provided in stages as it becomes available to Komatsu.

6.2 Komatsu shall co-operate with Customer and take such commercially reasonable steps to assist in the investigation, containment, and remediation of a Security Incident.

6.3 To the extent a Security Incident gives rise to a need to provide (i) notification to public authorities, individuals, or other persons, or (ii) undertake other remedial measures including, without limitation, notice, credit monitoring services, and/or the establishment of a call center to respond to inquiries, at Customer's request, Komatsu shall provide commercially reasonable assistance.

6.4 In the event of a Security Incident, Komatsu shall not inform any regulator without first obtaining Customer's prior consent, unless it is independently required to do so by a law to which Komatsu is subject, in which case Komatsu shall, to the extent permitted by such law (i) not refer to, or mention, Customer in any such information, and (ii) inform Customer of that legal requirement. For avoidance of doubt, Customer, as the Controller, retains the right and obligation to determine, in its sole discretion, whether notification of a Security Incident involving Customer Personal Data to Supervisory Authorities, individuals, or other persons is required.

6.5 Customer agrees that any notice by Komatsu of a Security Incident pursuant to this Section is not an admission of fault or liability on Komatsu's behalf. To the extent that a Security Incident is caused by Customer, Customer Affiliate, a Customer client, or anyone acting for Customer, Komatsu will inform the Customer of the Security Incident and provide information it discovers up to the stage it identifies the breach is caused by the Customer, Customer Affiliate, Customer client, or anyone acting for the Customer. Further assistance to investigate and remediate such a Security Incident is subject to the commercially reasonable prior agreement of the Parties acting in good faith and Komatsu reserves the right to charge Customer a reasonable administrative fee for assistance in such circumstances.

7. Assistance to Customer – Regulator Requests and Data Subject Rights

7.1 Taking into account the nature of the Processing and the information available to Komatsu, Komatsu shall promptly notify Customer if it receives any complaint, communication, subpoena, warrant, court order, audit notice, or other request ("request") from a Supervisory Authority, law enforcement, court, or tribunal in respect of Customer Personal Data. Komatsu shall not respond to the request itself, unless required by applicable law or authorized to do so by Customer. Komatsu shall cooperate with and assist Customer (i) in relation to a communication from a Regulator, public authority, law enforcement, representative labor body, or a Supervisory Authority, and (ii) in ensuring compliance with GDPR Articles 32-36 or equivalent obligations under applicable Data Protection Law. Where such assistance is unduly burdensome, Komatsu retains the right to charge Customer a reasonable administrative hourly fee to provide such assistance.

7.2 Komatsu shall promptly notify Customer in writing or electronically if Komatsu receives a request to exercise privacy rights from an individual relating to Customer Personal Data (a "**Privacy Rights Request**"). Komatsu shall not otherwise communicate with the requestor regarding the Privacy Rights Request unless the Customer directs Komatsu to do so, in which case Komatsu reserves the right to charge Customer a reasonable administrative fee to handle the Privacy Rights Request. Komatsu shall, in a manner consistent with the nature and functionality of the Services provided in the Agreement and Komatsu's role as a Processor, provide reasonable support to Customer to enable Customer to respond to a Privacy Rights Request, provided that Komatsu will provide such assistance to the extent:

7.2.1 the information is available to Komatsu, and such information is not otherwise available to Customer, or the requested assistance cannot practicably be performed by Customer; and

7.2.2 Customer acknowledges that Komatsu has no responsibility to interact directly with any individual or regulator in respect of any request, demand, or order (except as expressly provided under applicable Data Protection Law or as otherwise agreed by the Parties in writing).

8. Deletion or Return of Customer Personal Data

8.1 Subject to Section 8.2, and as required under applicable Data Protection Law, upon Customer's request Komatsu shall promptly: (a) return a copy of all Customer Personal Data to Customer by secure file transfer; and (b) delete all Customer Personal Data, other than Customer Personal Data stored in backup locations, which shall be deleted pursuant to Komatsu's backup and retention schedules. Subject to the foregoing, deletion of Customer Personal Data shall occur within 60 calendar days of termination of the Agreement.

8.2 Komatsu may retain Customer Personal Data to the extent and for such period as required by Data Protection Law, provided that Komatsu shall ensure the confidentiality of all such Customer Personal Data and ensure that such Customer Personal Data is only Processed for the purpose(s) specified in such law.

8.3 Notwithstanding anything in this DPA or the Agreement to the contrary, until Customer Personal Data is deleted or returned, Komatsu shall continue to comply with this DPA.

9. Audit Rights

9.1 Customer acknowledges that Komatsu is regularly audited against industry security standards by independent third-party auditors. Upon request, Komatsu shall supply Customer a summary of its most recent cybersecurity audit report(s), which reports shall be subject to the confidentiality provisions contained in the Agreement. Pursuant to applicable Data Protection Law, Customer, or its independent third-party auditor, may audit Komatsu's security practices only if:

9.1.1 Komatsu has been unable to provide sufficient evidence of its compliance with its obligations under this DPA or applicable Data Protection Law by providing summaries or copies of its independent audit reports, the sufficiency of which shall be based on a reasonable assessment by Customer;

9.1.2 An audit is formally requested by a Supervisory Authority or regulator; or

9.1.3 Applicable Data Protection Law confers on Customer such a right, provided that Customer shall not conduct such an audit more than once in any 12-month period, unless applicable Data Protection Law requires otherwise.

9.2 The rights set out in Section 9.1 will be exercised in accordance with the following principles:

9.2.1 any audit will be exercised taking a risk-based approach, considering the context and the nature of the Services, and adhering to relevant, commonly accepted audit standards;

9.2.2 if Customer appoints a third-party to exercise its audit rights, Customer will use reasonable efforts to verify that the third-party auditor's personnel have acquired the right skills and knowledge to perform effective

and relevant audits and assessments of the Services, and must ensure that such personnel are subject to binding confidentiality obligations;

9.2.3 audits will be restricted to survey or questionnaire style audits, and will not involve physical access to Komatsu's premises;

9.2.4 audits will be restricted to Komatsu's normal business hours, and will not unreasonably interfere with Komatsu's business operations; and

9.2.5 if the exercise of any audit right could, in Komatsu's reasonable opinion, create a risk for another Komatsu customer's environment, Customer and Komatsu (or the Regulator, as applicable), may agree on an alternative way to address the request to provide a similar level of assurance.

9.3 If an audit under this Section 9 results in a determination that Komatsu has not established reasonable and adequate security controls for compliance with Komatsu's obligations under this DPA, such a finding shall not constitute a breach of the DPA or the Agreement provided Komatsu remedies the deficiency within a reasonable period.

10. Restricted Transfers

10.1 Customer (as "data exporter") and Komatsu (as "data importer"), with effect from the commencement of the relevant transfer, hereby enter into: (i) the EU SCCs, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to GDPR (subject to Section 10.2); and (ii) the UK IDTA, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to UK Data Protection Law (subject to Section 10.3). Further, until such time as the relevant jurisdiction(s) issue their own standard contractual clauses, the relevant EU SCCs shall apply in respect of any Restricted Transfer subject to any other Data Protection Law that regulates cross-border transfers of Personal Data.

10.2 The Parties agree that, with respect to the EU SCCs:

10.2.1 *Clause 7 – Docking clause* shall not apply;

10.2.2 In *Clause 9 – Use of subprocessors*, Option 2 shall apply and the "time period" shall be thirty (30) days;

10.2.3 In *Clause 11(a) – Redress*, the optional language shall not apply;

10.2.4 In *Clause 13(a) – Supervision*, the following shall be inserted: 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 1.C**, shall act as competent supervisory authority.

10.2.5 In *Clause 17 – Governing law*, the "Member State" shall be Great Britain;

10.2.6 In *Clause 18 – Choice of forum and jurisdiction*, the Member State shall be Great Britain;

10.2.7 *Annex I* shall be deemed completed with the relevant sections of **Annex 1** to this DPA;

10.2.8 *Annex II* shall be deemed completed with the relevant sections of **Annex 2** to this DPA; and

10.2.9 *Annex III* shall be deemed completed with the relevant sections of **Annex 3** to this DPA.

10.3 In respect of Restricted Transfers from the UK, the SCCs (as incorporated by reference) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is as set forth below:

10.3.1 Table 1 – the Parties are Komatsu and Customer, with contact details as set forth in **Annex 1** to this DPA.

10.3.2 Table 2 – the Approved EU Standard Contractual Clauses with optional provisions as set forth in Section 10.2.

10.3.3 Table 3 – the Annexes are deemed completed with the relevant information contained in the Annexes to this DPA.

10.3.4 Table 4 – neither Party has the right of termination set forth in Section 19 of the UK IDTA.

10.4 The Parties agree that with respect to Swiss Personal Data the EU SCCs will apply amended and adapted as follows:

10.4.1 the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority;

10.4.2 the term "member state" must 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; and

10.4.3 references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced).

10.5 If Komatsu receives legal process requiring disclosure of Customer Personal Data to a public authority in a Third Country that does not benefit from an adequacy decision, Komatsu shall promptly, and as applicable: (i) inform the relevant public authority of the incompatibility of the legal process with the safeguards provided under this DPA, and the resulting conflict of obligations for Komatsu; (ii) promptly notify Customer of the legal process; (iii) assess the lawfulness of the legal process; (iv) respond to the legal process by using reasonable efforts to challenge the validity of the legal process where there are grounds to do so; (v) seek interim measures to suspend the effects of the legal process until the relevant court or authority has decided on the merits; (vi) refrain from disclosing the Customer Personal Data until required to do so under the applicable procedural rules; and (vii) provide the minimum amount of Customer Personal Data permissible when responding to the legal process, based on a reasonable interpretation thereof.

10.6 Komatsu shall inform Customer of developments that might lead to Komatsu's inability to comply with its obligations under this DPA (including the SCCs and the jurisdictional requirements set forth in Annex 4). In the event of any such change, Customer shall be entitled to immediately (i) suspend the transfer of Customer Personal Data, (ii) terminate this DPA, and/or (iii) require Komatsu to return or delete the Customer Personal Data.

11. Liability

11.1 Komatsu's limitations of, and exclusions from, liability are as set forth in the Agreement; provided that Komatsu shall not be liable for costs or damages incurred by Customer as a result of an action or inaction by Customer that causes or results in a Security Incident.

12. General Terms

12.1 Precedence. To the extent there is any conflict between the Agreement, this DPA, and/or the SCCs, the various agreements will control in the following order of preference: (i) the SCCs, (ii) this DPA, (iii) the Agreement. Annex 4 forms an integral part of this DPA. If there is any inconsistency between the exhibits incorporated via Annex 4 and any other provision of this DPA, the applicable exhibit shall prevail to the extent of the inconsistency, but only with respect to the jurisdiction-specific terms in the exhibit that apply to the Parties.

12.2 Survival. Any obligation imposed on Komatsu or any Komatsu Affiliate under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of this DPA.

12.3 Governing Law. This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects in accordance with the choice of law and jurisdiction clauses contained in the Agreement.

12.4 Forthcoming Changes to applicable Data Protection Law. Should the Parties become subject to new requirements under applicable Data Protection Laws, the Parties agree to comply with the provisions in this DPA to the extent applicable. Should new requirements under applicable Data Protection Laws require additional contractual obligations not provided for in this DPA, the Parties shall negotiate in good faith to implement such obligations, including, without limitation, by way of an amendment to this DPA made in writing.

AGREED AND ACKNOWLEDGED:

Modular Mining Systems Inc.	**Customer**
By: Signed by: Mark Schaeffer D3FE43AE71D145F...	By: _____
Title: VP Strategy	Title: _____
Date: 06 August 2026 | 10:41 AM MST	Date: _____

SEAL

ANNEX 1 – DESCRIPTION OF THE PROCESSING

A. LIST OF PARTIES

Data exporter(s):

1)	Name:	Customer's name as provided in the order form or applicable contract
	Address:	Customer's address as provided in the order form
	Contact person's name, position, and contact details:	Customer contact as provided in the order form
	Activities relevant to the data transferred under these Clauses:	Use of Komatsu's Services as described in the Agreement or order form.
	Role (controller/processor):	Controller

Data importer(s):

1)	Name:	Modular Mining Systems Inc.
	Address:	3289 E. Hemisphere Loop
	Contact person's name, position, and contact details:	Greg Karadjian, Director- Solutions Greg.Karadjian@global.komatsu
	Activities relevant to the data transferred under these Clauses:	Providing and supporting the Services as described in the Agreement.
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred / processed (delete or add as necessary)

- Customer's employees, contractors, and contingent workers.

Categories of Personal Data transferred / processed (delete or add as necessary)

- Operator logins
- Operator first and last name
- Operator ID number
- Customer email addresses
- Location data (i.e., tracking of equipment that may be associated with an operator)

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Unless otherwise agreed, the transferred Personal Data will not comprise special categories of Personal Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation.

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

- Transfers will be made on (select one):
  - ☒ continuous basis.
  - ☐ a one-off basis commencing on DATE and terminating on DATE.

Nature of the processing

- The nature of the processing (i.e., the Services provided) is as described in the Agreement.

Purpose(s) of the data transfer and further processing

- To provide the Services as described 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

- Customer Personal Data will be retained for the duration of the Agreement, after which point Komatsu will delete the Customer Personal Data unless otherwise required under applicable law.

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

- The subject matter and duration of the processing is as outlined above within this Annex. The nature of the specific subprocessing services is as further described in the Subprocessor list provided by Komatsu.

C. **COMPETENT SUPERVISORY AUTHORITY**

- The competent supervisory authority is as determined in accordance with Clause 13 of the Standard Contractual Clauses.

ANNEX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

Description of the technical and organizational 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:

Komatsu shall comply with the following Information Security Requirements:

Physical Access Control

	Technical Measures		**Organizational Measures**
X	Alarm system	X	Key regulation and current key list
X	Automatic access control system	X	Reception
	Biometric locking system	X	Visitor book/ visitor log
X	Chip cards/ transponder systems	X	Employee/ visitor identification
X	Manual locking system	X	Visitors accompanied by employee
X	Safety lock	X	Granting and revoking of access authorization is documented and reviewed periodically
	Locking system with code lock		Information, which includes paper documents, handled by the data importer is classified, labelled, protected, and handled accordingly
X	Securing building shafts	X	Documentation of the transfer of physical storage media
	Bell system with camera	X	Careful selection of the Security and Cleaning personnel.
X	Video surveillance		
X	Enclosure locks		

Logical Access Control

	Technical Measures		**Organizational Measures**
X	Screen lock with password activation in user's absence	X	"Clean desk" guidelines
X	Encryption of data media	X	Mobile device policy and management
X	Encrypted smartphones		Account lockout occurs on 3 failed authentication attempts, with an administrative alert raised
X	Encrypted laptops/tablets	X	General guidelines for data protection and/or security
X	Multi-Factor Authentication	X	Role-based authorization concept (read / write / change / copy / delete)

	Login with biometric data	X	Granting and revoking of access authorization is documented and reviewed periodically
	Enclosure locks	X	Authentication attempts are logged
X	BIOS protection (separate password)		
	Locks for external ports		
X	End Point Protection		
X	E-mails are automatically scanned by anti-virus and antispam software		

Separation Control

	Technical Measures		**Organizational Measures**
X	Logical separations (systems / databases)	X	Determination of database rights
X	Use of different types of encryptions	X	Control via permissions concept
X	Separation of productive and test environment		Datasets allocated purpose attributes

Pseudonymization

	Technical measures		**Organizational measures**
	Random generation of assignment tables or secret parameters used in an algorithmic pseudonymization		Definition of the pseudonymization rule, possibly based on personnel, customer, or patient identification numbers (use of UUID v4)
	In the case of pseudonymization separation of the assignment data and storage in separate and secure system (possibly encrypted)		Determination of persons authorized to manage the pseudonymization process, carry out pseudonymization and, if necessary, de -pseudonymization
X	Controlled destruction of data media		Internal instruction to anonymize/ pseudonymize personal data in case of transfer or even after expiry of the statutory cancellation period

Integrity – Disclosure Controls

	Technical Measures		**Organizational Measures**
X	Access and retrieval logs	X	Documentation of retrieval and transmission processes

N/A	Secure transport containers		Regulations regarding dispatch method and determination of transport route
X	Securing of the transmission and transport route	X	Care by selection of transport personnel and vehicles
	Encryption of data before it is stored on systems or before it is transferred to databases	X	Documentation of data recipients
N/A	Monitoring of transportation time	X	Personal handover with log
X	Encryption of database backups.	X	Notify in the event of an incident of a breach in security
	Email encryption		
X	Use of signature procedures		
	Consistently encrypted data transfer between systems		
	External access only via secure connections (VPN, RDP or similar). Please specify		
X	Availability via encrypted connections such as sftp, https		

Input Control

	Technical Measures		**Organizational Measures**
	Technical logging of input, editing and deletion of data		Overview of the data that can be inputted, edited, or deleted and the respective programs used for this
X	Manual or automatic control of logs		Traceability of input, editing and deletion of data by individual usernames (not user groups)
		X	Assignment of permissions to input, edit and delete data based on a permissions concept
		X	Retention of forms or logs from which data was extracted within automated processes
		X	Clear responsibilities for deletions
			Formalized Control frameworks and TPA to take care that not a single person can access, modify, or use critical information assets without authorization or detection

Availability and Resilience - Availability Control

	Technical Measures		**Organizational Measures**
X	UPS (Uninterrupted Power Supply)	X	Emergency responders are automatically contacted when fire detection systems are activated
X	Temperature and humidity levels of data are monitored and maintained at appropriate levels	X	The emergency plans are subject to a regular and continuous audit and improvement process
X	Emergency power system	X	Fire detection and suppression systems is certified at appropriate intervals
X	Fire protection and disaster regulations	X	Generators to support critical systems in the event of a power failure is certified at appropriate intervals
X	Fire and smoke alarm systems	X	Business continuity/disaster recovery plan policy for the restoration of critical processes and operations of the Supplier's services at the location(s) from which the Supplier's services is provided
X	Fire extinguisher in server room	X	Storage of backup media in a secure location outside the server room
X	RAID or similar technology for data redundancy		
	Video monitoring of server room		
	Alarm triggering upon unauthorized access to server room		
X	Virus protection concept		
X	Server room monitoring temperature and humidity		
X	Physical Protection measures in place for critical sites (surge protection, raised floors, cooling systems)		
X	Environmental control components are monitored and periodically tested		
	Data protection safe (S60DIS, S120DIS, other suitable standards with source seal etc.)		

Resilience & Rapid Recovery

	Technical Measures		**Organizational Measures**
	Regular disaster recovery tests and logging of the results for mechanisms for data recovery, protection against accidental destruction and loss		The plans are documented in service continuity and backup / recovery or emergency concepts
X	Software patches are tested and evaluated before they are installed in an operational environment. They are then introduced in regular intervals (please specify the intervals below)	X	Training employees to identify incidents and avoid future incidents
X	Intrusion detection and response system	X	Implementation of platform health monitoring tools with regular reviews to detect potential issues for early intervention
	Daily incremental data backup		
	Weekly complete data backup		
	Weekly backups on separately stored physical media or on physically separate systems		
X	Data redundancy through raw data backups in cloud storage blobs.		

Procedure for Regular Testing, Ranking and Evaluation

	Technical Measures		**Organizational Measures**
X	Software solutions for data protection management in use.	X	Formalized process for handling requests for information from data subjects is available
X	Central documentation of all procedures and regulations for data	X	Careful selection of the Contractor and Subcontractors personnel.
X	Protection with access for employees according to need/authorization.		Sanctions for breach of Agreement.
X	Other documented security concept (Two factor authentication)	X	An internal Data Protection Officer (Please provide a name/Company contact details)
X	A review of the effectiveness of the technical protection measures is performed at least once a year	X	Employees trained and committed to confidentiality/ data secrecy
	Safety certification e.g., ISO 27001	X	Regular awareness of employees, at least annually
		X	Internal/external information security officer
		X	Disciplinary measures in the event of data protection violations

			Work instructions on handling private data Procedures for Checking compliance with procedures and work instructions are in place
		X	The Privacy Impact Assessment (DSFA) is conducted as needed
			The company complies with the information obligations under Art. 13 and 14 GDPR

Incident Response Management

	Technical Measures		**Organizational Measures**
X	Security incidents are monitored and analyzed promptly by the Security Management organization	X	Documented procedure for handling security incidents
X	Use firewall and update regularly	X	Documentation of security incidents and data breaches
X	Intrusion detection systems	X	Formal process and responsibilities for post processing security incidents and data breaches
X	Use spam filter and update regularly	X	Contact method for internal parties to report potential incidents
X	Use virus scanner and update regularly	X	Management review and approval to major changes to internal organization occurs
X	Intrusion Prevention System	X	Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents are defined

Privacy by Design and Privacy by Default

	Technical Measures		**Organizational Measures**
X	No more personal information is collected than is necessary for the purpose	X	Logging and monitoring of proper execution of the Agreement
	Pseudo anonymize or encrypt data as early as possible	X	Controls are defined and documented for all known inherent priority risks in the business. For each of these controls are responsible defined to regularly monitor the effectiveness
	Delete or anonymize data as early as possible		Have a risk management process across all company levels and has appointed dedicated risk managers at various levels of the organization

X	Minimize access to data	X	Create appropriate transparency regarding procedures and processing of data
	IT systems are protected by a list of second-layer measures according to their security level identified during the risk analysis		Existing configuration options to the most privacy-friendly values
X	Simple exercise of the right of withdrawal of the person concerned by technical measures	X	Completion of the necessary order processing contract of EU standard contract clauses
		X	Written instructions to the contractor
		X	Selection of the contractor under due diligence
		X	Commitment of the contractor's employees to data secrecy
			Obligation to appoint a data protection officer by the contractor in case of existing order obligation
		X	Agreement on effective control rights vis-à-vis the contractor
		X	Subcontractors will be bound by the same rules and regulations as the Supplier

Order Control (Outsourcing to Third Parties)

	Technical Measures		**Organizational Measures**
		X	Prior checking of the security measures taken by the contractor and their documentation
		X	Selection of the contractor under due diligence (especially regarding data protection and data security)
			Completion of the necessary order processing contract or EU standard contract clauses
		X	Written instructions to the contractor
		X	Commitment of the contractor's employees to data secrecy
			Obligation to appoint a data protection officer by the contractor in case of existing order obligation
			Agreement on effective control rights vis-à-vis the contractor

			Regulation on the use of additional subcontractors
			Ensuring the destruction of data after completion of the contract
			For longer cooperation: ongoing verification of the contractor and his level of protection

Customer Responsibilities

Customer shall (i) ensure that Customer's approved users follow the same terms of service that apply to Customer; (ii) secure computer systems or devices in Customer's possession, custody, or control from threats that might impact the security, confidentiality, availability, and privacy of data; (iii) if Customer directs the use of data transfer tools or methods, Customer shall be responsible for securing the portion of the chain of custody that Customer controls, including any onward transfers Customer directs which are outside the control of Komatsu; (iv) direct the transfer of data between jurisdictions, including to approve or deny EU country to EU country data replication for disaster recovery and business continuity; (v) protect the confidentiality of each Customer user's login and password and managing each Customer user's access to the Services, and prohibiting the sharing of accounts and/or passwords; (vi) take appropriate action to secure, protect, and backup Customer Data in a manner that will provide appropriate security and protection, including encryption to protect Customer Data; and (vii) employ best practices to prevent uploading data containing malicious code into Komatsu's systems.

Subprocessors

Komatsu contractually requires its Subprocessors to take the same or substantially similar measures described in this Annex 2.

ANNEX 3 - SUBPROCESSORS

The controller has authorized the use of the Subprocessors found in its Subprocessor List:

Subprocessor Name:	**Data Storage Location:**	**Description of Processing:**
Microsoft Azure (and Azure AD)	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Cloud platform; Data storage; Data processing; CICD of data processing apps; authorization and permission implementation and management
Snowflake	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Data storage
DataDog	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Data storage; visualization tool
Confluent Cloud	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Data processing
Twilio	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Data processing
Databricks	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Data processing
Grafana Enterprise	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Data processing; visualization tool
Microsoft Power BI	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Visualization tool
Rapid7 – InsightIDR	West US, Central US, East US, North Central US, North Europe, West Europe, East Asia, Southeast Asia, Japan West, Japan East, Brazil South, Australia East, Australia Southeast	Security platform
Zendesk	United States (US East in Northern Virginia or Ohio, and US West in Oregon), European Economic Area	Customer support platform

	(EEA) (Ireland and Frankfurt), United Kingdom (UK), Japan (Tokyo or Osaka)	

ANNEX 4 – JURISDICTION-SPECIFIC REQUIREMENTS

The relevant Exhibits of this Annex 4 shall be applicable only where one or more Parties to this DPA are subject to the laws of the jurisdictions specified below:

Exhibit A – Brazil

Solely to the extent Komatsu Processes Personal Data that is subject to Brazil's Data Protection Law No. 13,709/2018, as may be amended or replaced, the following amendments shall apply:

1. Clause 5.1 is modified to delete the following language: "Komatsu will provide 30 days' notice prior to engaging a new Subprocessor. Should Customer reasonably object to the addition of a Subprocessor by Komatsu within the 30-day window, the parties shall negotiate in good faith to find a suitable alternative Subprocessor. If no agreement is reached between the parties, Customer shall have the right to terminate the Agreement as it relates to the use of the objected-to Subprocessor by Komatsu. Customer hereby consents to the Subprocessors listed in **Annex 3** hereto, subject to the conditions set out in Section 5.2."

2. Clause 10.1 is modified and replaced in its entirety to read as follows:

    a. "10.1. Customer (as "data exporter") and Komatsu (as "data importer"), with effect from the commencement of the relevant transfer, hereby enter into: (i) the EU SCCs, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to GDPR (subject to Section 10.2); and (ii) the UK IDTA, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to UK Data Protection Law (subject to Section 10.3); (iii) the Brazilian SCCs, which are expressly incorporated by reference herein, as if it had been set out in full, and automatically apply to the parties, in respect of any Restricted Transfer subject to Brazil's Data Protection Law No. 13,709/2018 (subject to Section 10.7). Further, until such time as the relevant jurisdiction(s) issue their own standard contractual clauses, the relevant EU SCCs shall apply in respect of any Restricted Transfer subject to any other Data Protection Law that regulates cross-border transfers of Personal Data."

3. Clause 10.7 is added as follows:

    10.7 "The parties agree that, with respect to the Brazilian SCCs:

    10.7.1 Clause 1.1: The Parties are identified in this DPA.

    10.7.2 Clause 2.1: The description of the international transfer is set out in **Annex 1** to this DPA.

    10.7.3 Clause 3: Option B shall apply, and the conditions of onward transfer are set out in **Annex 1** to this DPA.

    10.7.4 Clause 4: Option A shall apply.

    10.7.5 Clause 4.1:

    a. Responsible for publishing the document provided for in Clause 14;
        i. (X) Exporter ( ) Importer
    b. Responsible for responding to data subjects' requests as set forth in Clause 15:
        i. (X) Exporter ( ) Importer
    c. Responsible for reporting the security incident provided for in Clause 16:
        i. (X) Exporter ( ) Importer

    10.7.6 Section III: Details of security measures are set forth in **Annex 2** to this DPA."

Exhibit B – Canada

This Exhibit B applies to the Processing of Customer Personal Data solely to the extent such Processing is subject to the Data Protection Laws of Canada, whether federal or provincial (collectively, "**Canadian Data Protection Laws**"). In the event of any conflict between the main body of this DPA and this Exhibit B with respect to Processing activities subject to Canadian Data Protection Laws, the provisions of this Exhibit B shall prevail.

1. Definitions

For the purposes of Processing activities subject to Canadian Data Protection Laws, the following interpretive provisions shall apply:

a) "**Controller**" includes any person or entity that collects, uses, communicates, holds, or otherwise processes Personal Data for its own purposes (as opposed to doing so at the request, or under the direction of, another party);

b) "**Processor**" includes any person or entity that processes Personal Data at the request of or under the direction of another party (as opposed to its own purposes), including mandataries and service providers;

c) "**Personal Data**" includes "personal information" and any similar terms as may be defined under Canadian Data Protection Laws, and refers to any information relating to a natural person and that allows that person to be identified, whether directly or indirectly;

d) "**Security Incident**" includes "Confidentiality Incident" and any similar terms as may be defined under Canadian Data Protection Laws, and refers to any access, use, or communication of Personal Data not authorized by law, loss of Personal Data, or any other breach in the protection of Personal Data;

e) "**Processing**" shall include the collection, use, communication, disclosure, retention, deletion, or any other type of operation performed on Personal Data;

f) "**Sensitive Personal Data**" includes Personal Data that, due to its nature, in particular its medical, biometric, or otherwise intimate nature, or the context of its use or communication, entails a high level of reasonable expectation of privacy, or as otherwise specifically defined or considered as sensitive under Canadian Data Protection Laws;

g) "**Supervisory Authority**" includes the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the British Columbia Office of the Information and Privacy Commissioner, the Alberta Office of the Information and Privacy Commissioner, or any other applicable Canadian federal or provincial authority charged with the protection of Personal Data or the application of Canadian Data Protection Laws.

2. Cross-Border Transfer Requirements

For the purposes of Restricted Transfers subject to Canadian Data Protection Laws, the following provisions shall apply:

a) Customer represents and warrants that, to the extent required by applicable Canadian Data Protection Laws, all Canadian Data Subjects have been notified, at the time of collection, that their Personal Data may be transferred outside of their province or territory of residence.

b) In respect of any Restricted Transfer of Customer Personal Data originating from the province of Quebec, Canada, to another jurisdiction (which, for clarity, includes transfers to other Canadian provinces):

i. Customer (as "data exporter") shall, prior to any such Restricted Transfer, conduct an assessment of privacy-related factors compliant with the requirements of Quebec Data Protection Law, including, without limitation, Section 17 of the *Act Respecting the Protection of Personal Information in the Private Sector*, which assessment takes into account the sensitivity of the Customer Personal Data, the purposes for which the Customer Personal Data will be used, the protections (legal, contractual, or otherwise) that will be afforded to the Customer Personal Data, and the applicable privacy and data protection laws of the jurisdiction to which the Customer Personal Data will be transferred. Such transfers shall take place if Customer is satisfied that the Customer Personal Data will receive an adequate level of protection after the transfer is completed with regard to the requirements of Quebec Data Protection Law.

ii. Komatsu (as "data importer") shall provide reasonable assistance and cooperation to Customer in conducting any such privacy impact assessment, including providing information regarding the technical and organizational measures in place for the protection of Customer Personal Data and any relevant information regarding applicable laws in the jurisdiction in which Komatsu will be Processing such Customer Personal Data; and

iii. Komatsu shall implement any measures identified in such assessment that are reasonably necessary to ensure that the transferred Customer Personal Data will receive an adequate degree of protection within the meaning of applicable Data Protection Laws, notwithstanding the transfer.

c) In the event of a change in applicable Canadian Data Protection Laws which is likely to have a substantial effect on the parties' obligations relating to Restricted Transfers subject to Canadian Data Protection Laws, the parties shall collaborate and work together in good faith to agree any steps which have to be taken to allow Komatsu, as data importer, to continue processing Customer Personal Data in compliance with applicable Canadian Data Protection Laws, the Agreement, the DPA, and this Exhibit.

3. Security Incidents

With respect to a Security Incident involving Customer Personal Data subject to Canadian Data Protection Laws, without limiting any of the obligations set out in Section 6 of the DPA, Komatsu shall notify Customer without undue delay (but after a reasonable period to allow Komatsu to investigate and, if necessary, involve law enforcement) upon Komatsu becoming aware of (i) a Security Incident and (ii) to the extent required by applicable Canadian Data Protection Laws, any violation or attempted violation by any person of any obligation concerning the confidentiality of the Customer Personal Data communicated to Komatsu.

4. Consent Withdrawal.

With respect to Customer Personal Data subject to Canadian Data Protection Laws, if a Data Subject withdraws consent to the Processing of their Personal Data, Customer shall notify Komatsu of such withdrawal without delay, and Komatsu shall cease Processing the relevant Personal Data and, where required by applicable Canadian Data Protection Laws, delete such Personal Data.

5. Governing Law.

In respect of processing activities subject to Canadian Data Protection Laws, the provisions of this Exhibit B shall be governed by the laws applicable in the Canadian province in which such processing activities take place or from which the Customer Personal Data originates, as applicable.

Exhibit C – Australia

Solely to the extent Komatsu Processes Personal Data that is subject to Australia's Privacy Act 1988 (Cth), as may be amended or replaced, the following amendments shall apply:

1. Clause 1.2.12 is deleted and replaced with " "**Sensitive Personal Data**" means Sensitive Information, as that term is defined in the *Privacy Act 1988* (Cth)."

2. Clause 1.2.15 is deleted and replaced with " "**Third Country**" means any country outside of Australia."

3. Clause 2.4.1 is deleted and replaced with "process Customer Personal Data only for the specific purposes of the Processing as set out in **Annex 1** or as otherwise instructed by Customer, unless Processing is required by Data Protection Law or other law to which the Komatsu is subject, in which case Komatsu shall inform Customer of that legal requirement before such Processing, unless that law prohibits disclosure of such information;"

4. Clause 3.2 is deleted and replaced with "Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Without limitation, Customer shall ensure that the Customer Personal Data is or has been collected in accordance with the Data Protection Laws, and that Data Subjects have been notified of all matters of which they are required or entitled to be notified of under Data Protection Laws at the time their Personal Data is collected. Customer represents that its use of the Services will not violate the rights of any individual that has opted-out from the Sale or Sharing of, or other disclosure of, Customer Personal Data, to the extent applicable under Data Protection Law."

5. Clause 6.4 is deleted and replaced with "In the event of a Security Incident, Komatsu shall not inform or correspond with any regulator or individual about that Security Incident without first obtaining Customer's prior consent, unless required by a law to which Komatsu is subject or if the Customer does not otherwise notify any regulator or individuals in accordance with its obligations under applicable Data Protection Law, in which case Komatsu shall, to the extent permitted by such law (i) not refer to, or mention, Customer in any such information, and (ii) inform Customer of that legal requirement. For avoidance of doubt, Customer, as the Controller, retains the right and obligation to determine, in its sole discretion, whether notification of a Security Incident involving Customer Personal Data to Supervisory Authorities, individuals, or other persons is required, and bears responsibility for making such notifications in accordance with applicable Data Protection Law."

6. Clause 7.2 is deleted and replaced with "Komatsu shall promptly notify Customer in writing if Komatsu receives a request to exercise privacy rights or complaint from an individual relating to Customer Personal Data (a "Privacy Rights Request"). Komatsu shall not otherwise communicate with the requestor regarding the Privacy Rights Request unless the Customer directs Komatsu to do so or if the Customer does not otherwise respond to a Privacy Rights Request in accordance with its obligations under applicable Data Protection Law, in which case Komatsu reserves the right to charge Customer a reasonable administrative fee to handle the Privacy Rights Request. For avoidance of doubt, Customer bears responsibility for responding to Privacy Rights Requests in accordance with applicable Data Protection Law."

7. Clause 8.1 is deleted and replaced with "Subject to Section 8.2, and as required under applicable Data Protection Law, upon Customer's request Komatsu shall promptly: (a) return a copy of all Customer Personal Data to Customer by secure file transfer; and (b) delete or deidentify all Customer Personal Data, other than Customer Personal Data stored in backup locations, which shall be deleted pursuant to Komatsu's backup and retention schedules. Subject to the foregoing, deletion or deidentification of Customer Personal Data shall occur within 60 calendar days of termination or expiry of the Agreement."

8. Clause 8.3 is deleted and replaced with "Notwithstanding anything in this DPA or the Agreement to the contrary, until Customer Personal Data is deleted, deidentified, or returned, Komatsu shall continue to comply with this DPA."

Exhibit D – India

Solely to the extent Komatsu Processes Personal Data that is subject to India's Digital Personal Data Protection Act, as may be amended or replaced, the following amendments shall apply:

1. Clause 6.4 is deleted and replaced with: "In the event of a Security Incident, Komatsu may inform any regulator without first obtaining Customer's prior consent, in which case Komatsu shall, to the extent permitted by such law (i) not refer to, or mention, Customer in any such information, and (ii) inform Customer of that legal requirement."

2. Clause 10.7 is added as follows: "To the extent that Personal Data collected from Customers in India is being transferred to any other jurisdiction, the Parties will ensure that such Personal Data is being transferred in accordance with any standards prescribed under applicable Data Protection Laws and is not transferred to a country to which applicable Data Protection Laws prohibit such transfer."

3. Clause 12.1 of the DPA is deleted and replaced with: "Precedence. To the extent there is any conflict between the Agreement or this DPA, the various agreements will control in the following order of preference: (i) this DPA, and (ii) the Agreement. Annex 4 forms an integral part of this DPA. If there is any inconsistency between the exhibits incorporated via Annex 4 and any other provision of this DPA, the applicable exhibit shall prevail to the extent of the inconsistency, but only with respect to the jurisdiction-specific terms in the exhibit that apply to the Parties."

4. Annex 1, Paragraph C of the DPA pertaining to competent supervisory authority will not apply.

Exhibit E – South Africa

Solely to the extent Komatsu Processes Personal Data that is subject to South Africa's Protection of Personal Information Act, 2013, as may be amended or replaced, the following amendments shall apply:

1. **Definitions**. The following definitions shall supplement or replace (as applicable) the definitions section of the DPA:

    a. Clause 1 is hereby amended by the inclusion of the following definitions:
        i. "**Controller**" shall include a "responsible party" as defined under POPIA.

        ii. "**Data Subject**" means the person to whom Personal Data relates and shall include natural persons and, where it is applicable, an existing juristic person.

        iii. "**Personal Data**" shall include "personal information" as defined under POPIA and includes personal information of natural persons as well as juristic persons, where applicable.

        iv. "**POPIA**" shall mean the Protection of Personal Information Act, 4 of 2013 as amended or replaced from time to time and the regulations thereto.

        v. "**Processor**" shall include an "operator" as defined under POPIA.

        vi. "**Supervisory Authority**" shall include the "Regulator" as defined under POPIA.

    b. Clause 1 is hereby amended to include the following additional wording to the following definitions in clause 1:

        i. "**Security Incident**" shall include a security compromise as contemplated in POPIA and accordingly includes a situation where there are reasonable grounds to believe that the Personal Data of a Data Subject has been accessed or acquired by any unauthorised person.

        ii. "**Sensitive Personal Data**" shall include special personal information as defined under POPIA.

2. **Processor Obligations**. Clause 2.3 shall be amended by the inclusion of the following at the end of clause 2.3: "Furthermore, Customer hereby consents to Komatsu transferring Customer Personal Data to a location outside South Africa and, where applicable, Customer undertakes to procure the consent of its respective clients or customers to the transfer of their Personal Data to countries outside of South Africa."

3. **Customer Obligations.** Clause 3.2 shall be amended by the deletion of the word "individual" and the replacement of that word with "Data Subject".

4. **Restricted Transfers.** The following wording shall be added to the end of Clause 10.1 *(Restricted Transfers):*

    a. For purposes of compliance with POPIA, Customer Personal Data that falls within the ambit of POPIA may not be transferred from South Africa to other countries unless: (a) the country to which the Customer Personal Data is transferred has adequate data protection laws that uphold data protection principles similar to those contained in POPIA, including the provisions relating to further transfers of Personal Data; or (b) an appropriate binding agreement has been concluded with the recipient of the Customer Personal Data which requires the recipient to uphold data protection principles substantially similar to those contained in this Data Processing Addendum. Any further transfer of such Customer Personal Data shall require compliance with all the provisions in this Data Processing Addendum.