JBT Corporation
OmniBlu™ System Data Processing Agreement

1. BACKGROUND AND DETAILS OF THE PERSONAL DATA PROCESSING

1.1 This Data Processing Agreement ("DPA") supplements the Contract between Buyer and the John Bean Technologies business entity that is party to the Contract ("JBT Contracting Party" or "JBT"). This DPA applies whenever the JBT Contracting Party, its employees or (sub)contractors may process Personal Data on behalf of Buyer. This shall particularly include the processing of the categories of Personal Data relating to the data subjects and for the purposes as listed in **Attachment 1** to this DPA.

1.2. The scope and duration, as well as the extent and nature of the collection, processing and use of Personal Data under this DPA shall be as defined in the applicable Contract.

1.3 The term of this DPA corresponds to the duration of the Contract.

2. DEFINITIONS

In addition to the definitions set out in the applicable Contract, the following definitions shall apply in this DPA:

Contract: means the Sales Order, Sales Contract, Services Agreement and any other agreement under which JBT provides services to Data Controller and under which JBT processes data on behalf of Data Controller through the OmniBlu™ System.

Data Controller: means the relevant Buyer or customer which (i) has entered into a Contract with JBT as processor which refers to this DPA by reference, or which (ii) has otherwise agreed to the provision of Personal Data processing services of JBT as the processor to which this DPA shall apply.

DPA: means this Data Processing Agreement.

EEA: means the European Economic Area.

Standard Contractual Clauses: means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the EU GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from module two of such clauses and as further set out in Clause 8 of this DPA ("EU Standard Contractual Clauses"). In respect of UK Personal Data, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner ("ICO") and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by Section 17 of such Addendum, the parties agree to change the format of the information set out in Part 1 (Tables) of the Addendum as further set out in Clause 8 of this DPA (the "UK Addendum"). The Standard Contractual Clauses also mean any future clauses issued by the EU or the ICO for the transfer of Personal Data to non-EU or non-UK (sub)processors, and replacing or modifying the clause in the wording as issued by the EU or the ICO, or any other clauses mutually agreed by the parties. In case of such modification or replacement, **Attachments 1, 2 and 3** to this DPA shall remain attachments to the Standard Contractual Clauses.

EU GDPR: means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

GDPR: means the EU GDPR and UK GDPR, as applicable.

In writing: includes electronic text form such as email, pdf or fax.

Personal Data: means personal data as defined in the GDPR and to the extent processed by JBT on behalf of Data Controller when providing services under the Contract.

Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Any terms used in this DPA, which are defined in the GDPR and not otherwise defined in this DPA, shall have the meaning as set out in the GDPR.

UK GDPR: means the GDPR as applicable as part of UK domestic law by virtue 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 (as amended).

3. INSTRUCTIONS OF DATA CONTROLLERS

3.1 JBT will follow instructions received from Data Controller with respect to Personal Data.

3.2 Data Controller instructs JBT to collect, process and use Personal Data to provide the services as agreed in the Contract.

3.3 Additional instructions may be issued by Data Controller. Such instructions should be provided in advance and in writing by Data Controller, subject to Processor's right to charge additional sums at its current rates should the scope of the agreed services be exceeded.

3.4 JBT shall inform Data Controller if it considers an instruction to violate the GDPR or other EU or EU Member State data protection provisions.

4. OBLIGATIONS OF JBT

4.1 JBT shall not use the Data Controllers' Personal Data for any purpose other than described in the Contract and to fulfil its obligations under the Contract, unless required to do so by European Union or EU Member State law to which JBT is subject; in such a case, JBT shall inform Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 JBT Personnel

4.2.1 JBT's personnel engaged in performing processing operations under this DPA have been bound to confidentiality and are prohibited from accessing, processing and/or using any Personal Data without authorization and for purposes other than fulfilling JBT's contractual obligations vis-à-vis Data Controller.

4.2.2 JBT will familiarize all individuals having access to the Data Controllers' Personal Data with the data protection provisions relevant to their work.

4.3 At Data Controller's request and cost and taking into account the nature of processing and the information available to JBT, it will assist Data Controller with its obligations under Articles 32 to 36 of the GDPR.

5. DATA SUBJECT'S RIGHTS

5.1 Taking into account the nature of the processing, JBT will assist Data Controller at Data Controller's request and cost with Data Controller's obligation to respond to requests from data subjects seeking to exercise their rights under the GDPR. JBT may do so by implementing appropriate technical and organizational measures and by providing further assistance to the extent that such Personal Data is not already accessible to Data Controller through the services.

5.2 JBT will inform Data Controller without undue delay if a data subject contacts JBT directly with a request as described in Articles 12 to 22 of the GDPR.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

6.1 JBT will implement and maintain the technical and organizational measures set out in **Attachment 2** to this DPA.

6.2 Upon Data Controller's request, JBT will provide evidence of such technical and organizational measures through (i) current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor), or (ii) a suitable certification of IT security or data protection auditing (e.g. ISO/IEC 27001).

6.3 The technical and organizational measures are subject to technical progress and further development. JBT may amend the technical and organizational measures, provided that the new measures do not fall short of the general level of security described in Attachment 2.

7. COMMUNICATION IN THE CASE OF PERSONAL DATA BREACHES

7.1 JBT shall notify Data Controller without undue delay if JBT becomes aware of any Security Breach. Notifications made pursuant to this section will describe, to the extent reasonably possible, details of the Security Breach, including steps taken to mitigate the potential risks and steps JBT recommends the Data Controllers take to address the Security Breach.

7.2 Data Controller instructs JBT to take measures JBT deems necessary or helpful to secure the Personal Data processed on behalf of Data Controller and to minimize possible adverse consequences to the data subjects.

7.3 JBT shall be liable for Data Protection Losses, as defined in Section 7.1 of this Agreement, (howsoever arising whether in contract, tort (including negligence) or otherwise) under or in connection with this Agreement (i) only to the extent caused by the processing of Personal Data by JBT and/or its subprocessors under this Agreement and directly resulting from a breach of JBT's obligations under this Agreement; and (ii) in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this Agreement, or in case of gross negligence or willful intent by the Data Controller. JBT's liability for damages suffered the Data Controller are capped at the annual value of the Contract and excludes liability for lost profits and indirect or consequential damages, such as but not limited to loss of revenue, loss of opportunity and loss of goodwill. No limitation of liability shall apply in case of gross negligence of willful intent by JBT, its employees, contractors, subprocessors and representatives.

8. INTERNATIONAL TRANSFERS

8.1 Where the GDPR applies to the Personal Data processed under this DPA and JBT is an entity established in the EEA or the UK, then JBT relies on its intragroup data transfer agreement, including the Standard Contractual Clauses (and the processor-processor Module, 3), for the international transfer of aforementioned Personal Data.

8.2 Where the GDPR applies to the Personal Data processed under this DPA and JBT is not an entity established in the EEA or the UK, then:

a) the EU Standard Contractual Clauses are incorporated by reference insofar the aforementioned Personal Data is subject to international data transfer rules under the EU GDPR; and/or

b) the UK Standard Contractual Clauses are incorporated by reference insofar the aforementioned Personal Data is subject to international data transfer rules under the UK GDPR.

8.3 For the purpose of the EU Standard Contractual Clauses, the following shall apply: (i) the optional Clause 7 (Docking Clause) and the second paragraph of Clause 11(a) (Redress) will not be included, (ii) option 2 (General Written Authorization) of Clause 9a (Use of sub-processors) will be applicable and the notification time period mentioned there will be the same as described in Clause 9 of this DPA, (iii) the clauses shall be governed by the laws of the Netherlands (Clause 17: Governing law) and (iv) the courts of the Netherlands shall have jurisdiction (Clause 18: Choice of forum and jurisdiction).

8.4 For the purposes of the UK Addendum, the following shall apply: (i) details of the parties in table 1 shall be as set out in **Attachment 1** to this DPA (with no requirement for signature), (ii) for the purposes of table 2 the UK Addendum shall be appended to the EU Standard Contractual Clauses (including the selection of module(s) and application/disapplication of optional clauses as noted above), (iii) the appendix information as listed in table 3 is set out in **Attachments 1** (Annex IA and IB) **2** and **3** to this DPA and (iv) for the purposes of table 4, JBT and Data Controller may end the UK Addendum as set out in Section 19 thereof.

9. SUBPROCESSING

9.1 The JBT Contracting Party may hire third parties or engage its affiliates to provide certain limited or ancillary services on its behalf. Data Controller consents to the engagement of JBT's affiliates and the third parties mentioned in **Attachment 3** as subprocessors.

9.2 From time to time, the JBT Contracting Party may engage new subprocessors. JBT Contracting Party will give Data Controller notice (by updating its website and provide Data Controller with a mechanism to obtain notice of that update / sending Data Controller) of any new subprocessor at least fifteen (15) days in advance of providing that subprocessor with access to Data Controller or Personal Data.

9.3 If Data Controller does not approve of a new subprocessor, then Data Controller may terminate any subscription for the affected service without penalty by providing, before the end of the relevant notice period, written notice of termination that includes an explanation of the grounds for non-approval.

9.4. The JBT Contracting Party shall remain responsible for its subprocessor's compliance with the obligations of this DPA and any subprocessor to whom the JBT Contracting Party transfers Personal Data, even those used for storage purposes, will have entered into written agreements with the JBT Contracting Party that provide at least the same level of protection as this DPA, in particular containing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the such subprocessing will meet the requirements of the GDPR.

9.5. Except as set forth in the DPA, or as Data Controller may otherwise authorize in writing, the JBT Contracting Party will not transfer to any third party (not even for storage purposes) Personal Data that Data Controller provided to the JBT Contracting Party for the purpose described in the Contract. The Data Controller consents to the transfer of Personal Data to subprocessors, including affiliates of the JBT Contracting Party, as set out in **Attachment 3**.

9.6. JBT shall ensure that when it transfers Personal Data from the EEA and/or the UK to its affiliates and subprocessors located in countries outside the EEA and/or the UK, such transfers will be governed by the EU Standard Contractual Clauses, any other adequate safeguards as mentioned in Article 46 of the GDPR and/or the UK Addendum, unless the transfer is to a country covered by a valid adequacy determination by a competent authority with jurisdiction over the Data Controller.

10. AUDIT RIGHTS

10.1 Audit

10.1.1 The Data Controller may conduct an audit to verify JBT's compliance with its obligations under this DPA if the Data Controller in its reasonable discretion believes that the right under section 6.2 above is not sufficient in an individual case, a competent data protection authority requests it, or the circumstances of a Security Breach require an earlier audit. Such audit may be conducted by the Data Controller or a third party auditor. JBT shall reasonably cooperate and provide such documentation and access as reasonably required by the Data Controller to conduct the audit. For the avoidance of doubt, JBT shall in no event be obliged to provide any information related to other customers. JBT may claim remuneration for its efforts when enabling Data Controller audits, on a time and material basis and general rates in line with the market standard within this area.

10.1.2 Reasonable advance written notice of at least fifteen (15) days is required for any such audit with JBT, unless: (i) data protection law or a competent data protection authority require an earlier audit, in which case JBT will be given as much advance notice as possible; or (ii) the circumstances of a Security Breach require an earlier audit, in which case JBT will be given reasonable advance notice. The Data Controller shall conduct the audit in an expeditious manner during normal business hours, within a reasonable time and in a way so as not to unreasonably disrupt JBT's day-to-day business operations, in particular without any impact on the general IT security of JBT.

10.1.3 If an audit determines that JBT has breached its obligations under this DPA, JBT will promptly remedy the breach at its own cost.

10.2 Evidence

10.2.1 Upon request, JBT will certify to the Data Controller that it is in compliance with this DPA by providing adequate evidence in the form of (i) the results of a self-audit, (ii) internal company rules of conduct including external evidence of compliance, (iii) certificates on data protection and/or information security (e. g. ISO 27001), (iv) approved codes of conduct, or (v) other appropriate certificates.

10.2.2 Evidence of the implementation of measures which are not specific to this DPA may be given in the form of up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit.

11. DELETION OF PERSONAL DATA

11.1 Following termination or expiry of the Contract and upon first request by Data Controller, JBT shall delete or return to Data Controller any Personal Data it processed for Data Controller under the Contract, unless European Union or EU Member State law requires storage of the Personal Data. In absence of any such request, JBT shall delete the Personal Data ninety (90) days after the aforementioned termination or expiry.

12. MISCELLANEOUS

12.1 In the event of any contradictions, the provisions of this DPA shall take precedence over the provisions of the Contract.

ATTACHMENT 1
CATEGORIES OF PERSONAL DATA, CATEGORIES OF DATA SUBJECTS AND PURPOSE OF COLLECTION, PROCESSING AND USE OF PERSONAL DATA

This Attachment forms part of the DPA and must be completed by the parties.

A. LIST OF PARTIES

Data Controller
The Data Controller is the customer receiving the IT support and data processing services from JBT as described in the Contract. To enable this, JBT may store and access Personal Data controlled by the Data Controller and which is contained in IT systems for which JBT provides support to Data Controller.

The Data Controller, Buyer, is the Data Exporter insofar Section 8.2 of the DPA applies.
Processor
The processor is JBT which renders IT support and data processing services.

The processor, JBT, is the Data Importer insofar Section 8.2 of the DPA applies.

B. DESCRIPTION OF PROCESSING (AND TRANSFER IF APPLICABLE)

Data subjects
The Personal Data may concern the following categories of data subjects:

- Employees and other staff of Data Controller
- Any other persons whose personal data are processed by JBT on behalf of Data Controller.

Categories of data
The Personal Data concern the following categories of data:

- Machine and User logs
- Login credentials
- Contact details
- Any other Personal Data which are processed by JBT on behalf of Data Controller.

Special categories of data (if appropriate)
The Personal Data concern the following special categories of data:

- None

Processing operations (nature and purpose)
The Personal Data will be subject to the following basic processing activities and (if applicable) will be transferred for the following purposes:

- IT support as described in the Contract
- Hosting of dashboards and web applications as described in the Contract

If applicable, the frequency of the sharing of data and the transfer thereof

- The data is transferred on a continuous basis

The period for which the data will be retained or the criteria used to determine the period

- The Personal Data will be retained as long as the duration of the Contract and will be deleted as described in the DPA

C. COMPETENT SUPERVISORY AUTHORITY (EU STANDARD CONTRACTUAL CLAUSES ONLY)

Data exporter is established in an EEA country. The competent supervisory authority is the authority of the EEA country (or where applicable: federal state/region within such EEA country) in which data exporter is established.

ATTACHMENT 2
TECHNICAL AND ORGANIZATIONAL MEASURES

JBT’s administrative, physical, organizational and technical measures shall include, at a minimum, the following:

Documentation and accountability
Implementation of accountability principles and documentation of operations related to data processing and data security, This is accomplished through:

- Drafting, implementing and monitoring an extensive company-wide IT Security Policy and Standards for IT Assets; and
- Applying Confidentiality and Non-Disclosure Agreements where appropriate and as described in JBT Policies.

Access control of processing areas
Implementation of suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment used to process the Personal Data. This is accomplished through:

- Keys and card key systems;
- Receptionists and building security; and
- CCTV.

Access control to data processing systems
Implementation of suitable measures to prevent data processing systems from being used by unauthorized persons. This is accomplished through:

- Individual user ID's and strong passwords subject to minimum security requirements for staff members;
- Mandatory password changes on regular intervals;
- Acceptable use policies for IT Assets such as PC's and mobile phones and applications;
- Strict on- and off-boarding policies for staff members;
- Lock out of user accounts after a limited number of failed log-in attempts; and
- Advanced firewalls, PEN testing, anti-virus and spam scanning.

Access control to use specific areas of data processing systems
The persons entitled to use its data processing systems are only able to access the data within scope and to the extent covered by their respective access permission (authorization) and that the Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- Access management on strict need-to-know principles, job duties, project responsibilities and actual business activities; and
- Strict VPN corporate network requirements.

Transmission control
Implementation of suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged. This is accomplished by:

- Firewall and encryption technologies to protect gateways through which the data travels; and
- Monitoring of encryption technologies.

Access and input control
Implementation of suitable measures to ensure that it is possible to check and establish whether, when, by whom and for what reason Personal Data have been input into data processing systems or otherwise processed. This is accomplished by:

- Authentication of the authorized users via user ID and passwords;
- Restricted physical access to processing areas; and
- System time-out after non-activity for a pre-determined time period.

Instructional control
Personal data may only be processed in accordance with the DPA and Data Controller’s instructions. This is accomplished by:

- Information & security training and policies & procedures for staff.

Availability control
Implementing suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- Business continuity, backup and disaster recovery management; and
- Offsite backup storage.

Separation of processing for different purposes

Implementing suitable measures to ensure that Personal Data that are intended for different purposes can be processed separately. This is accomplished by:

- Access to Personal Data being restricted via user authorization passwords;
- Function separation of Personal Data of different customers; and
- Use of Personal Data being application specific.

ATTACHMENT 3
LIST OF SUBPROCESSORS

Data Controller consents to JBT engaging the following sub-contractors:

Subprocessor (full legal name)	Address/country	Description of services provided by the subprocessors
Microsoft Corporation	One Microsoft Way, Redmond, WA 98052, United States	Provision of Azure cloud services host the Portal.
Google	1600 Amphitheatre Parkway Mountain View, CA 94043	Analytics services
Twilio/Sendgrid	375 Beale Street Suite 300 San Francisco, CA 94105 USA	Notification Services