# JBT Corporation
# OmniBlu™ 系统数据处理协议

**1.个人数据处理的背景及详情**

1.1 本数据处理协议（下称 "DPA"）是买方与作为合同一方的 John Bean Technologies 业务实体（下称“JBT 缔约方”或 "JBT"）之间的合同的补充。当 JBT 缔约方、其员工或承包商（分包商）代表买方处理个人数据时，本 DPA 即适用。尤其包括为本 DPA **附件 1** 所列目的处理与该附件所列数据主体相关的各类个人数据。

1.2.本 DPA 项下个人数据的收集、处理和使用的范围和时长，以及程度和性质应在相应合同中定义。

1.3 本 DPA 的期限与合同的期限相对应。

**2.定义**

除适用合同中所述的定义外，以下定义应适用于本 DPA：

合同：指销售订单、销售合同、服务协议和任何其他协议，在这些协议项下 JBT 向数据控制方提供服务且 JBT 代表数据控制方通过 OmniBlu™ 系统处理数据。

数据控制方：指以下相关买方或客户：(i)已与作为处理方的 JBT 订立合同，且该合同援引了本 DPA，或 (ii)以其他方式同意 JBT 作为处理方提供个人数据处理服务，且适用本 DPA。

DPA：指本数据处理协议。

EEA：指欧洲经济区。

标准合同条款：指欧盟委员会以(EU) 2021/914 号委员会实施决定通过的，根据欧盟一般数据保护条例 (GDPR)将个人数据传输到第三国的标准合同条款，包括该等条款模块二的文本，本 DPA 第 8 条中有进一步阐述（下称“欧盟标准合同条款”）。就英国的个人数据而言，信息专员办公室 ("ICO") 于 2022 年 2 月 2 日根据 2018 年数据保护法第 119a 条发布欧盟标准合同条款的国际数据传输附录并提交给议会，但是，根据该附录第 17 条，双方同意按照本 DPA 第 8 条所述，更改附录第 1 部分（表格）中所列信息的格式（下称“英国附录”）。标准合同条款还指欧盟或 ICO 今后发布的关于将个人数据传输至非欧盟或非英国的（次级）处理方的任何条款，以及取代或修改欧盟或 ICO 发布的措辞中的条款，或双方协商一致的任何其他条款。如有此类修改或取代，本 DPA 的**附件 1、2 和 3** 仍应作为标准合同条款的附件。

欧盟 GDPR：指欧洲议会和理事会于 2016 年 4 月 27 日通过的，关于在个人数据处理和此类数据自由流动方面保护自然人以及废止 95/46/EC 号指令的(EU) 2016/679 号条例（一般数据保护条例）。

GDPR：指欧盟 GDPR 和英国 GDPR（如适用）。

书面形式：包括电子文本形式，如电子邮件，PDF 或传真。

个人数据：指 GDPR 中定义的个人数据，并在 JBT 根据合同提供服务时代表数据控制方所处理的范围内。

安全事件：指任何安全事故，而导致所传输、存储或以其他方式处理的个人数据的意外或非法损毁、丢失、被篡改、遭致未经授权的披露或访问。

本 DPA 中使用的任何在 GDPR 中已定义而在此未另外定义的术语，应具有 GDPR 所述的含义。

英国 GDPR：指根据 2018 年欧盟（退出）法案第 3 节，并被 2019 年数据保护、隐私和电子通讯（脱欧）条例（修正案等）所修订的，作为英国国内法的一部分而适用的 GDPR（被不时修订）。

**3.数据控制方的指示**

3.1 JBT 应遵守所收到的来自数据控制方的关于个人数据的指示。

3.2 数据控制方指示 JBT 收集、处理和使用个人数据，以提供合同中约定的服务。

3.3 数据控制方可发出额外指示。数据控制方应提前以书面形式提供此类指示，而处理方有权在超过约定服务范围时按其现行费率收取额外费用。

3.4 如果 JBT 认为指示违反 GDPR 或其他欧盟或欧盟成员国的数据保护条款，则应通知数据控制方。

**4.JBT 的义务**

4.1 JBT 不得将数据控制方的个人数据用于合同所述以外以及履行合同义务以外的任何目的，除非 JBT 所遵循的欧盟或欧盟成员国法律要求这样做；在此情况下，JBT 应在处理前将该法律要求告知数据控制方，除非该法律基于公共利益的重要理由禁止此等披露。

4.2 JBT 员工

4.2.1 执行本 DPA 项下处理操作的 JBT 员工负有保密义务，禁止在未经授权的情况下出于履行 JBT 对数据控制方的合同义务以外的目的访问、处理和/或使用任何个人数据。

4.2.2 JBT 应让有权访问数据控制方的个人数据的所有员工熟悉与其工作相关的数据保护条款。

4.3 应数据控制方要求并考虑到处理的性质和对 JBT 可用的信息，JBT 应协助数据控制方履行 GDPR 第 32 至 36 条规定的义务，成本由数据控制方承担。

**5.数据主体的权利**

5.1 考虑到处理的性质，应数据控制方要求且由数据控制方承担成本，JBT 应协助数据控制方履行其义务，以响应数据主体寻求行使 GDPR 项下权利的要求。为此，JBT 应落实适当的技术和组织措施，并在数据控制方无法通过服务访问该等个人数据时提供进一步的协助。

5.2 如果数据主体直接联系 JBT 并提出 GDPR 第 12 至 22 条所述的要求，JBT 应通知数据控制方而不得有不当迟延。

**6.技术和组织措施**

6.1 JBT 应落实并维持本 DPA **附件 2** 所述的技术和组织措施。

6.2 应数据控制方要求，JBT 应通过以下方式提供此类技术和组织措施的证据：(i) 当前审计师的证书、由独立机构（如审计师、数据保护官、IT 安全部门、数据隐私审计师、质量审计师）提供的报告或报告节选，或 (ii) IT 安全或数据保护审计的适当认证（如 ISO/IEC 27001）。

6.3 该等技术和组织措施受到技术进步和进一步发展的影响。JBT 可调整技术和组织措施，前提是新措施不低于附件 2 所述的一般安全水平。

**7.发生个人数据事件时的沟通**

7.1 如果 JBT 意识到任何安全事件，应通知数据控制方而不得有不当迟延。根据本节发出的通知应在尽可能合理的范围内描述安全事件的详情，包括为减轻潜在风险而采取的措施，以及 JBT 建议数据控制方为处理安全事件而采取的措施。

7.2 数据控制方指示 JBT 采取 JBT 认为必要或有益的措施，以确保其代表数据控制方所处理的个人数据的安全，并尽量减少对数据主体可能造成的不利后果。

**8.国际传输**

8.1 如果 GDPR 适用于本 DPA 项下所处理的个人数据，且 JBT 是在欧洲经济区或英国设立的实体，则 JBT 遵循其集团内部数据传输协议，包括标准合同条款（处理方-处理方，即模块 3），以进行上述个人数据的国际传输。

8.2 如果 GDPR 适用于本 DPA 项下所处理的个人数据，但 JBT 不是在欧洲经济区或英国设立的实体，则：

a) 在上述个人数据受欧盟 GDPR 的国际数据传输规则约束的情况下，欧盟标准合同条款将被援引合并到本 DPA 中；及/或

b) 在上述个人数据受英国 GDPR 的国际数据传输规则约束的情况下，英国标准合同条款将被援引合并到本 DPA 中。

8.3 就欧盟标准合同条款而言，以下几点适用：(i) 可选第 7 条（对接条款）和第 11 (a) 条（补救）的第二段将不会包含在内，(ii) 第 9a 条（使用次级处理方）的选项 2（通用书面授权）将适用，其中所述通知时间期限与本 DPA 第 9 条所述一致，(iii) 该条款受荷兰法律管辖（第 17 条：适用法律），(iv) 荷兰法院享有管辖权（第 18 条：法院和司法管辖区的选择)。

8.4 就英国附录而言，以下几点适用：(i) 表 1 中双方的详情应在本 DPA **附件 1** 中列出（无需签名），(ii) 就表 2 而言，英国附录应增补至欧盟标准合同条款（包括模块的选择和上述可选条款的适用/不予适用），(iii) 表 3 所列的附录信息载于本 DPA **附件 1**（附录 IA 及 IB）、**附件 2** 和**附件 3** 中，以及 (iv) 就表 4 而言，JBT 和数据控制方可按照第 19 节所述终止英国附录。

**9.次级处理**

9.1 JBT 缔约方可以雇用第三方或聘请其关联公司代表其提供某些限定或辅助性的服务。数据控制方同意聘请 JBT 关联公司和**附件 3** 所述的第三方作为次级处理方。

9.2 JBT 缔约方可能不时聘请新的次级处理方。JBT 缔约方应在向新的次级处理方提供访问数据控制方或个人数据的权限之前至少十五 (15) 天，向数据控制方发出相应的通知（通过更新其网站，并向数据控制方提供获得该更新的通知的途径，或发送至数据控制方）。

9.3 如果数据控制方未批准新的次级处理方，则数据控制方可在相关通知期限结束之前，提供书面终止通知（包括对不批准理由的解释）以终止对受影响服务的订阅，而不受任何处罚。

9.4 JBT 缔约方应保持对其次级处理方遵守本 DPA 的义务而负责，JBT 缔约方向其传输个人数据的任何次级处理方（即使是用于存储目的）需与 JBT 缔约方订立书面协议，承诺提供至少与本 DPA 相同水平的保护，特别是应充分保证以适当的方式落实适当的技术和组织措施，以便该等次级处理操作符合 GDPR 的要求。

9.5 除非 DPA 中有规定，或数据控制方另行书面授权，否则 JBT 缔约方不得将数据控制方为合同中所述目的提供给 JBT 缔约方的个人数据传输给任何第三方（即使是为了存储目的）。数据控制方同意将个人数据传输给**附件 3** 所列的次级处理方，包括 JBT 缔约方的关联公司。

9.6 JBT 应确保，当其将个人数据从欧洲经济区和/或英国传输至其位于欧洲经济区和/或英国以外国家的关联公司和次级处理方时，该等传输将受欧盟标准合同条款、GDPR 第 46 条和/或英国附录中提到的任何其他充分保障措施的约束，除非系传输至经对数据控制方具有管辖权的主管当局作出的有效的充分性决定涵盖的国家。

**10.审计权利**

10.1 审计

10.1.1 如果数据控制方基于合理的自由裁量认为上述第 6.2 条规定的权利在个别情况下不够充分，应主管数据保护机构要求，或者因安全事件需要开展提前审计，则数据控制方可开展审计，以验证 JBT 是否遵守本 DPA 项下的义务。此类审计可由数据控制方或第三方审计师开展。JBT 应予以合理配合，并提供数据控制方为进行审计而合理要求的文件和权限。为避免疑义，JBT 在任何情况下均没有义务提供与其他客户有关的任何信息。JBT 可针对其配合数据控制方开展审计的工作，以时间和材料为基础根据符合该领域市场标准的一般费率要求报酬。

10.1.2 对 JBT 开展的任何此类审计均需提前至少十五 (15) 天发出合理的书面通知，以下情况除外：(i) 数据保护法或主管数据保护机构要求提前进行审计，在此情况下，将尽早通知 JBT；或 (ii) 因安全事件需要提前进行审计，在此情况下，将向 JBT 发出合理的事先通知。数据控制方应在正常营业期间，在合理的时间内快速开展审计，避免干扰 JBT 日常业务运营，特别是不得影响 JBT 的一般 IT 安全。

10.1.3 如果审计确定 JBT 违反本 DPA 项下的义务，JBT 应立即纠正违约并自行承担费用。

10.2 证据

10.2.1 应要求，JBT 应通过以下方式提供充分的证据，向数据控制方证明其遵守本 DPA：(i) 自我审计结果，(ii) 公司内部行为规则，包括外部的合规证据，(iii) 数据保护和/或信息安全证书（例如 ISO 27001），(iv) 经批准的行为准则，或 (v) 其他适当的证书。

10.2.2 非具体针对本 DPA 的措施的实施证据可以以独立机构（例如外部审计师、内部审计、数据保护官、IT 安全部门或质量审计师）的最新认证、报告或摘要的形式提供，或 IT 安全或数据保护审计的适当认证的形式提供。

**11.个人数据的删除**

11.1 合同终止或期满后，在数据控制方首次提出要求时，JBT 应删除或向数据控制方返还其根据合同为数据控制方所处理的任何个人数据，除非欧盟或欧盟成员国法律要求存储个人数据。如无任何此类要求，JBT 应在上述终止或期满后九十 (90) 天内删除个人数据。

**12.其他**

12.1 如有任何冲突，本 DPA 的条款应优先于合同的条款。

**附件 1**

**个人数据的类别、数据主体的类别及收集、处理及使用个人数据之目的**

本附件构成 DPA 的一部分，必须由双方共同填写。

**A. 协议双方列表**

**数据控制方**
数据控制方是合同所述接受来自 JBT 的 IT 支持和数据处理服务的客户。为提供服务，JBT 可能存储和访问由数据控制方控制的个人数据，这些数据包含在 JBT 为数据控制方提供支持的 IT 系统中。

*数据控制方，即买方，是 DPA 第 8.2 条适用范围内的数据输出方。*

**处理方**
处理方是指提供 IT 支持和数据处理服务的 JBT。

*处理方，即 JBT，是 DPA 第 8.2 条适用范围内的数据输入方。*

**B. 处理（及传输，若适用）的描述**

**数据主体**
个人数据可能涉及以下类别的数据主体：
- 数据控制方的雇员和其他员工
- JBT 代表数据控制方处理其个人数据的任何其他人。

**数据类别**
个人数据涉及以下类别的数据：
- 机器和用户日志
- 登录凭据
- 联系信息详情
- JBT 代表数据控制方处理的任何其他个人数据。

**特殊的数据类别（如适用）**
个人数据涉及以下特殊类别的数据：
- 无

**处理操作（性质和目的）**
个人数据将被用于以下基本处理活动，并为以下目的而被传输（如适用）：
- 合同所述的 IT 支持
- 合同所述的控制面板和 Web 应用程序托管

**若适用，数据共享和传输的频率**
- 数据将被连续传输

**数据保留的期限或用于确定期限的标准**
- 个人数据将在合同有效期内保留，并将按照 DPA 所述予以删除

**C. 主管监管机构（仅适用于欧盟标准合同条款）**

数据输出方系在欧洲经济区 (EEA) 国家设立。主管监管机构是数据输出方所设立的 EEA 国家（或若适用：该 EEA 国家的联邦、州/地区）的当局。

**附件 2**
**技术和组织措施**

JBT 的管理、物理、组织和技术措施应至少包括以下内容：

**记录和问责**
落实与数据处理和数据安全相关的问责原则和操作记录。具体办法为：
- 起草、执行并监测广泛的全公司范围内的 IT 安全政策和 IT 资产标准；以及
- 必要时适用 JBT 政策所述的保密和不披露协议。

**处理区域的访问控制**
采取适当措施，防止未经授权的人员访问用于处理个人数据的数据处理设备。 具体办法为：
- 密钥和卡片密钥系统；
- 前台及楼宇安保；以及
- 闭路电视。

**数据处理系统的访问控制**
采取适当措施，防止未经授权的人员使用数据处理系统。 具体办法为：
- 为工作人员设置个人用户 ID 和符合最低安全要求的强密码；
- 定期强制更改密码；
- 落实可接受的 IT 资产（如个人电脑、手机和应用程序）使用政策；
- 对工作人员执行严格的入职和离职政策；
- 在有限次数的失败登录尝试后锁定用户帐号；以及
- 高级防火墙、渗透测试、杀毒和垃圾邮件扫描。

**对使用数据处理系统的特定范围的访问控制**
有权使用（JBT）数据处理系统的人员仅可在各自的访问权限（授权）所涵盖的范围内访问数据，且未经授权不得读取、复制、修改或删除个人数据。 具体办法为：
- 根据严格的需知原则、工作职责、项目职责和实际业务活动进行访问管理；以及
- 执行严格的 VPN 企业网络要求。

**传输控制**
采取适当措施，防止个人数据在传输过程中或在数据媒体的运送过程中被未经授权的一方读取、复制、更改或删除，并确保可检查并明确通过数据传输设施将个人数据传输至哪些机构。 具体办法为：
- 采用防火墙和加密技术，以保护数据传输的网关；以及
- 监测加密技术。

**访问和输入控制**
采取适当措施，以确保可检查并明确个人数据是否、何时、由谁以及出于何种原因被输入数据处理系统或以其他方式被处理。 具体办法为：
- 通过用户 ID 和密码验证授权用户的身份；
- 限制进入处理区域；以及
- 在预先确定的时间段内无活动后系统暂停。

**指示控制**
个人数据仅可按照 DPA 和数据控制方的指示进行处理。 具体办法为：
- 落实针对员工的信息和安全培训以及执行政策和程序。

**可用性控制**
采取适当措施，确保个人数据不会意外损毁或丢失。 具体办法为：
- 实施业务连续性、备份和灾难恢复管理；以及
- 开展异地备份存储。

**针对不同用途进行分别处理**

采取适当措施，以确保针对不同用途的个人数据可分别处理。 具体办法为：

- 通过用户授权密码限制对个人数据的访问；
- 对不同客户的个人数据进行功能分离；以及
- 对个人数据的使用需针对特定应用。

**附件 3**
**次级处理方清单**

数据控制方同意 JBT 聘请以下分包商：

| 次级处理方（完整的法定名称） | 地址/国家 | 次级处理方提供的服务的描述 |
|---|---|---|
| Microsoft Corporation | One Microsoft Way, Redmond, WA 98052, United States | 提供 Azure 云端托管服务，托管门户。 |
| Google | 1600 Amphitheatre Parkway Mountain View, CA 94043 | 分析服务 |
| Twilio/Sendgrid | 375 Beale Street<br>Suite 300<br>San Francisco, CA 94105<br>USA | 通知服务 |