[Text Highlighted in Yellow Requires Review and Updating]

Note 1: the following clauses have been identified as the minimum items that need to be present in in order to comply with general Data Privacy regulations. Each of them needs to be compared to the document that is being amended to include the right references. Please read each statement carefully.

Note 2: If the transfers are only out of the UK and not the EEA, it may be necessary to create a new amendment for these transfers. Please contact dataprivacy@dieboldnixdorf.com if you believe this scenario applies to your contract.

Note 3: Mentions to the specific Data Processing Agreements/Documents are referred to as "this agreement". However, the nomenclature may vary in each contract; please consider if modifications are necessary.

Note 4: Please contact dataprivacy@dieboldnixdorf.com if your current contract does not identify: Subject Matter of Processing; Nature and Purpose of Processing; Duration of Processing; Categories of Company Personal Data; and/or Types of Data Subjects;

Amendment No. [xxx]
To the XXX Agreement

This Amendment No. [xxx] to the Agreement ("**Amendment**") is made as of [Date] (the **Effective Date**") by and between Diebold Nixdorf, Inc., 50 Executive Parkway, Hudson, Ohio 44236, United States of America (the "**Company**") and [Vendor Contracting Party and address] ("**Vendor**").

Company and Vendor are hereinafter referred to jointly as the "**Parties**" and each individually as a "**Party**."

RECITALS

WHEREAS, Company and Vendor entered into a Agreement dated [Date] ("**Agreement**");

WHEREAS, the Company has changed its permanent address;

WHEREAS, the Agreement may include certain exhibits, appendices, schedules, attachments, and other such transaction documents containing clauses regarding the processing of personal data ("**Data Processing Documents**");

WHEREAS, Company and Vendor desire to amend the Agreement and such Data Processing Documents;

NOW, THEREFORE, in consideration of the foregoing, the Parties hereto, intending to be legally bound, agree to amend the Agreement as follows:

1. The Company hereby notifies the Vendor of its change of address, which shall now be: 50 Executive Parkway, Hudson, Ohio 44236, United States of America.

2. The provisions set out in the underlying Data Processing Documents are hereby amended an replaced in accordance with the terms of Appendix 1 to this Amendment.

3. This Amendment is intended by the Parties to be the final expression of their agreement in this matter, and it constitutes the full and entire understanding between the Parties with respect to the subject hereof.

4. In the event of a conflict between the terms of this Amendment and the Agreement, including its Data Processing Documents, this Amendment shall control. All other terms and conditions of the Agreement shall remain in full force and effect and are unchanged by this Amendment.

5. If any provision of this Amendment or the application of any such provision shall be held contrary to law, the remaining provisions shall remain in full force and effect.

6. All capitalized terms used herein and not otherwise defined shall have the meaning ascribed to them under the terms of the Agreement.

IN WITNESS WHEREOF, Company and Vendor have executed this Amendment on the date set forth below their respective signature to be effective as of the Effective Date.

Customer:	Diebold Nixdorf	Vendor:
By:		By:
Name:		Name:
Title:		Title:
Date:		Date:

Appendix 1

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is executed between [Diebold entity], [Address] ("**Company**") and [Vendor name][Address] ("**Vendor**"). Company and Vendor are hereinafter referred to jointly as the "**Parties**" and each individually as a "**Party**."

Company and Vendor are entering into this DPA further to the underlying services agreement (the "**Agreement**") relevant to Vendor's provision of the Services (as defined below). The Parties have agreed to enter into this DPA for purposes of compliance with Data Protection Laws (as defined below). The DPA forms an integral part of the Agreement and all capitalized terms not defined herein shall have the meaning set forth in the Agreement.

The DPA is effective as of _____ (the "**Effective Date**").

1. Definitions.

The following definitions shall apply for this DPA:

"**Binding Corporate Rules**" means binding corporate rules that have been approved by the competent Supervisory Authority in accordance with Data Protection Laws and that are applicable to the provision of the Services.

"**Business**," "**Business Purpose**," "**Sell**" and "**Service Provider**" shall have the meanings given to them in the CCPA.

"**CCPA**" means California Civil Code Sec. 17981.100 *et seq* (also known as the California Consumer Privacy Act of 2018) and its implementing regulations as may be updated or amended from time to time.

"**Company Personal Data**" means all Personal Data (i) provided by (or on behalf) of Company to Vendor at any time in connection with or incidental to the Services, (ii) Processed at any time by the Vendor in connection with or incidental to the Services, or (iii) derived or generated by Vendor from the information described in (i) or (ii).

"**Controller**" (or such similar term under Data Protection Laws) means the entity that determines alone or jointly with others the purposes and means of Processing Personal Data.

"**Data Protection Laws**" means all worldwide laws and regulations applicable to Company, Vendor and/or the Services relating to (i) privacy and data security, and (ii) the use, collection, retention, storage, security, disclosure, transfer, disposal and other Processing of Company Personal Data, including without limitation European Data Protection Laws and the CCPA, in all cases as such laws and regulations may be amended, supplemented or replaced from time to time.

"**Data Subject**" means an identified or identifiable person to whom Personal Data relates.

"**Data Subject Request**" means a communication from a Data Subject regarding the exercise of rights pursuant to Data Protection Laws or an inquiry or complaint from a Data Subject related to the Processing of Company Personal Data.

"**European Data Protection Laws**" means all laws and regulations applicable to Company, Vendor or the Services relating to (i) privacy, data protection and data security; and (ii) the use, collection, retention, storage, security, disclosure, transfer, disposal and other Processing of Company Personal Data in Europe, including, without limitation, (a) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), (b) any European Economic Area ("**EEA**") Member State data protection law implementing or supplementing the GDPR, (c) the United Kingdom General Data Protection Regulation and UK Data Protection Act 2018 (together, "**UK Data Protection Laws**"), and (e) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance, in all cases as such laws and regulations may be amended, supplemented or replaced, from time to time.

"**Personal Data**" means any information relating to an identified or identifiable individual. It also includes any information protected similarly as "personal data," "personal information," "personally identifiable information" or such similar terms under Data Protection Laws.

"**Personal Data Breach**" means any actual or reasonably suspected breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, Company Personal Data or breach of security of Vendor's or its Suprocessors' systems Processing Company Personal Data. Personal Data Breach shall also have the meaning assigned by Data Protection Laws to the terms "security incident," "security breach, "personal data breach" or such similar terms.

"**Personnel**" means the employees of Vendor, including its permanent employees, fixed-term contract employees or temporary workers.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" (or such similar term under Data Protection Laws) means the entity that Processes Personal Data on behalf of the Controller.

"**Response-Related Costs**" means Company's internal and external costs relating to a Personal Data Breach, including, without limitation, (i) preparation and mailing or other transmission of legally required notifications; (ii) preparation and mailing or other transmission of such other communications to customers, agents, employees or others as Company deems reasonably appropriate; (iii) establishment of a call center or other communications procedures in response to such Personal Data Breach; (iv) public relations and other similar crisis management services; (v) forensic investigation, legal counsel, and accounting fees and expenses associated with Company's investigation of and response to such event; (vi) costs for credit monitoring services that are associated with legally required notifications or advisable under the circumstances; and (vii) court costs, fees and expenses of attorneys, accountants and other experts and all other fees and expenses of litigation or other proceedings.

"**Services**" means the services and other activities that Vendor shall provide or carry out for Company as set forth in the Agreement.

"**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to third countries approved pursuant to Commission Decision (EU) 2021/914 of 4 June 2021, found at ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

"**Subprocessor**" means another Processor engaged by Vendor to Process Company Personal Data, in accordance with Company's instructions.

"**Supervisory Authority**" means an independent public authority responsible for monitoring the application of Data Protection Laws, including the Processing of Personal Data covered by this DPA.

2. **Scope and Operation.**

2.1. This DPA applies to Vendor's Processing of Company Personal Data in the provision of the Services to Company in accordance with the Agreement. In this context:

2.1.1. Where Data Protection Laws provide for the roles of "Controller" and "Processor," Company acts as Controller of Company Personal Data and Vendor acts as Processor of Company Personal Data.

2.1.2. With respect to Company Personal Data of California residents, Company acts as a Business and Vendor acts as a Service Provider. Company is engaging Vendor to Process Company Personal Data of California residents on its behalf and in furtherance of one or more enumerated Business Purposes.

2.2. A description of the Processing of Company Personal Data related to the Services is set out in Annex 1. The description includes the subject matter, nature and purpose of Processing; the duration of the Processing; the categories of Company Personal Data and types of Data Subjects. Vendor shall not Process Company Personal Data for any other purpose than set out in Annex 1.

2.3. Vendor shall comply with Data Protection Laws when Processing Company Personal Data.

2.4. Vendor and any Subprocessor acting under its authority shall only Process Personal Data upon Company's documented instructions, unless, with respect to Personal Data of EEA or United Kingdom ("**UK**") Data Subjects, otherwise required by EU/EEA Member State law or UK law, respectively. In either case, Vendor shall inform Company of the relevant legal requirement prior to such Processing, unless Vendor is legally prohibited from informing Company of the requirement.

2.5. Vendor shall immediately inform Company if, in Vendor's opinion, Company's instructions infringe Data Protection Laws.

2.6. Vendor shall (i) not retain, use or disclose Company Personal Data for any purpose other than performing the Services for Company as specified in the Agreement, and (ii) not Sell Company Personal Data nor retain, use or disclose Company Personal Data outside of its direct business relationship with Company. Vendor understands the restrictions explicitly set forth in Cal. Civil Code 17981.140(w)(2)(A) and certifies that it will comply with such restrictions with respect to the Company Personal Data of California residents.

2.7. If Vendor becomes aware that Company Personal Data it is Processing is inaccurate, or has become outdated, it shall notify Company without undue delay and cooperate with Company to erase or rectify such Company Personal Data.

3. **Security Measures.**

3.1. In performing the Services, Vendor shall, at a minimum:

3.1.1. Develop, implement, maintain, monitor and update (as necessary) a comprehensive, written information security program applicable to the protection of the security, confidentiality, integrity and availability of Company Personal Data;

3.1.2. Implement technical and organizational measures to ensure a level of security appropriate to the risk associated with the Processing, including, at a minimum, the measures referred to in Data Protection Laws, and to protect Company Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Company Personal Data;

3.1.3. Implement and maintain appropriate security measures in accordance with good industry practice in the country or countries in which Vendor is Processing Company Personal Data and in accordance with the requirements of Data Protection Laws;

3.1.4. Use encryption methods to safeguard Company Personal Data while in transit;

3.1.5. Regularly monitor compliance with such security safeguards and ensure that there is no material decrease in the level of security afforded to Company Personal Data during the duration of the Processing; and

3.1.6. Provide timely updates to Company of any changes to the technical and organizational measures applicable to the Processing of Company Personal Data.

3.2. Annex 2 to this DPA describes the technical and organizational measures that Vendor has implemented with respect to the Processing of Company Personal Data.

4. **Confidentiality.**

4.1. Vendor shall keep all Company Personal Data and this DPA confidential.

4.2. Vendor shall limit access to Company Personal Data to Personnel who require such access in order to perform the Services. Any such access to Company Personal Data shall be granted on a strict "need to know" basis.

4.3. Vendor shall ensure that persons authorized to Process Company Personal Data have received appropriate training on their responsibilities and have executed written confidentiality agreements. Vendor shall ensure that such commitments to confidentiality endure through the duration of the Processing and after termination or conclusion of Processing.

5. **Subprocessing**.

5.1. Vendor shall not engage any Subprocessor or disclose any Company Personal Data to any third party without Company's prior specific written authorization. Vendor shall submit the request for specific authorization to Company (by email to dataprivacy@dieboldnixdorf.com) at least one month in advance of its engagement of a new Subprocessor. The request to engage a new Subprocessor should include (i) the identity of the new Subprocessor, (ii) the location in which the Subprocessor would Process Company Personal Data, (iii) a description of the relevant Processing operations to be carried out by the Subprocessor, and (iv) any other information reasonably requested by Company.

5.2. To the extent that Company authorizes Vendor to engage a Subprocessor ("**Authorized Subprocessor**"):

5.2.1. Vendor shall evaluate the security, privacy and confidentiality practices of each Authorized Subprocessor to establish that such Subprocessor is capable of providing the level of protection required by this DPA;

5.2.2. Vendor shall ensure that each Authorized Subprocessor is bound by a written agreement that at a minimum, binds Authorized Subprocessor to the same data protection obligations as those applicable to Vendor under this DPA. Such agreement must also include a third-party beneficiary clause whereby, in the event Vendor factually disappears, ceases to exist in law or becomes insolvent, Company shall have the right to terminate Vendor's agreement with Authorized Subprocessor and instruct Authorized Subprocessor to destroy or return Company Personal Data to Company. Vendor shall be responsible for ensuring Authorized Subprocessors comply with the obligations set forth in such agreement and Data Protection Laws;

5.2.3. Any cross-border transfers of Company Personal Data from Vendor to Authorized Subprocessors must comply with Data Protection Laws and where required, utilize appropriate transfer mechanisms; and

5.2.4. Vendor shall notify Company when its Authorized Subprocessor appoints a Subprocessor to Process Company Personal Data and comply with the requirements set out in this Section 5 of the DPA.

5.3. Upon request, Vendor shall provide (i) a list of Subprocessors to Company, and (ii) a copy of agreements with Subprocessors and any subsequent amendments thereto. Vendor may redact such agreements to the extent necessary to protect business secrets, other confidential information and Personal Data.

5.4. Vendor shall remain fully liable to Company for the performance of each Subprocessor's obligations in accordance with this DPA. Vendor shall notify Company of any failure by a Subprocessor to fulfill its contractual obligations.

6. **Data Subject Requests**.

6.1. Vendor shall, without undue delay, and in any event within one business day, notify Company (by email at dataprivacy@dieboldnixdorf.com) if it receives a Data Subject Request. Vendor shall not respond to any Data Subject Request, unless expressly instructed by Company.

6.2. Vendor shall provide all reasonable assistance to Company, including but not limited to providing requested information and/or deleting certain Company Personal Data, to ensure Company is compliant with its obligations under Data Protection Laws. Vendor shall comply with Company instructions when fulfilling its obligations under Section 6 of this DPA.

6.3. If Company requests information from Vendor to respond to a Data Subject Request, Vendor shall provide the requested information without undue delay, and in any event within three business days of Company's request. Vendor shall notify Company immediately if Vendor is unable to comply with the request for assistance. Such notification shall provide a detailed explanation as to why Vendor considers compliance with the request for assistance to be impossible.

6.4. In response to a Data Subject Request, Vendor shall provide Company Personal Data in a structured, commonly used, electronic, and machine-readable format or in such format as otherwise reasonably requested by Company.

7. **Personal Data Breach.**

7.1. Vendor shall without undue delay, and at the latest, within 24 hours after becoming aware of a Personal Data Breach, notify Company of the Personal Data Breach in writing, with a copy to informationsecurity@dieboldnixdorf.com. Such notification shall include: (i) a description of the nature of the Personal Data Breach (including the categories and approximate number of Data Subjects and data records concerned), (ii) the likely consequences of the Personal Data Breach, and (iii) the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects. If such information is not available at the time of initial notification, Vendor may provide such information to Company in a phased manner as the information becomes available.

7.2. Vendor shall immediately take action to contain such Personal Data Breach and mitigate potential risks to affected Data Subjects. Vendor shall keep Company advised of the status of the Personal Data Breach.

7.3. Vendor shall provide all assistance and cooperation reasonably requested by Company, in furtherance of (i) any correction, remediation, or investigation of a Personal Data Breach and/or the mitigation of any damage, (ii) any action Company may be required to take regarding a Personal Data Breach to comply with Data Protection Laws, including notifications to Supervisory Authorities and/or Data Subjects, and (iii) any actions that Company deems appropriate in relation to the Personal Data Breach, including the provision of any credit reporting services to affected Data Subjects.

7.4. Vendor shall not communicate with any third party (including any Data Subjects or regulatory authorities) regarding any Personal Data Breach, unless and until expressly instructed to do so by Company, or where required by law.

7.5. All remediation shall be at Vendor's expense and in accordance with Data Protection Laws. Vendor shall reimburse Company for all Response-Related Costs incurred by Company arising out of or in connection with a Personal Data Breach. Vendor shall cooperate at its own expense with Company in any litigation or other action deemed necessary by Company in relation to a Personal Data Breach.

8. **Audits and Inspections.**

8.1. Upon request, Vendor shall make available to Company any information Company may require (including information about Subprocessors) for purposes of demonstrating compliance with Company's obligations under this DPA and Data Protection Laws. Upon request, Vendor shall supply Company with a copy of its most recent internal or third-party audits and/or certifications pertaining to security, availability, processing integrity, confidentiality and privacy, including but not limited to certificates issued for the ISO 27000 series, the System and Organization Controls (SOC) 1 Report and the System and Organization Controls (SOC) 2 Type 2 Report. Vendor shall also complete security questionnaires provided by Company and commit to remediation efforts of any gaps identified upon review by Company.

8.2. Vendor shall allow for and contribute to audits conducted by Company or another auditor instructed by Company. If Vendor believes any request for information or cooperation pursuant to this DPA may infringe Data Protection Laws, it shall immediately notify Company in writing.

8.3. If requested by a Supervisory Authority, Vendor authorizes Company to share with such Supervisory Authority (i) any information Vendor provides pursuant to this DPA, and (ii) the results of any audit Company conducts pursuant to Section 8 of this DPA.

9. **Data Transfers**.

OPTION 1:

9.1. [The Parties acknowledge that neither Vendor nor any Subprocesor will transfer Company Personal Data from the EEA, UK or Switzerland to a country outside the EEA, UK or Switzerland in the performance of the Services.]

OPTION 2:

9.1. Vendor shall not transfer, or cause to be transferred, Company Personal Data from one country to another without Company's prior written consent. Where Company consents to such transfer, the transfer shall be in accordance with Data Protection Laws. Vendor shall provide an adequate level of protection for Company Personal Data wherever Processed in accordance with Data Protection Laws and this DPA.

9.2. Transfers of Company Personal Data from EEA/UK/Switzerland:

9.2.1. Annex 3 lists the locations where Company Personal Data will be Processed by Vendor and any Subprocessors. Subject to Section 9.2.2, the Standard Contractual Clauses shall apply to Customer Personal Data that is transferred to any Third Country. The Parties shall comply with the Controller-to-Processor Standard Contractual Clauses (Module 2), subject to the additional terms in Annex 4. Subject to Section 9.2.2, Vendor shall also enter into Standard Contractual Clauses for onward transfers of Company Personal Data with Subprocessors Processing Company Personal Data outside the EEA, UK and Switzerland.

9.2.2. The Standard Contractual Clauses shall not apply to Customer Personal Data that is transferred to a country deemed adequate by the European Commission (or by the UK Parliament with respect to transfers of Company Personal Data from the UK) or to any Third Country if Binding Corporate Rules or an alternative recognized compliance standard under Data Protection Law has been implemented for such transfer.

9.2.3. Vendor shall assist Company with completing any assessments for transfers of Company Personal Data outside of the EEA, UK and/or Switzerland, including by providing any information reasonably requested by Company related to a Subprocessor. The Parties agree to work together to implement safeguards for transfers of Company Personal Data to Third Countries that Company deems necessary to ensure such transfer is in compliance with Data Protection Laws.

9.3. In the event that any of the data transfer mechanisms set forth in this Section 9 of this DPA are amended, replaced, repealed or invalidated, the Parties shall work together in good faith to implement a valid transfer mechanism under Data Protection Laws, provide assurances as required under Data Protection Laws, and/or negotiate a solution to enable transfers of Company Personal Data that comply with Data Protection Laws.

10. **Sharing Company Personal Data with Third Parties**.

10.1. Vendor shall not disclose or provide access to any Company Personal Data to law enforcement or any other third party unless required by law. If Vendor is contacted with a demand for Company Personal Data, Vendor shall (i) attempt to redirect the law enforcement agency or other third party to request the Company Personal Data directly from Company, (ii) reject the request or demand unless required by law to comply, and (iii)

promptly notify Company and provide Company a copy of the request or demand unless legally prohibited from doing so. If Vendor is compelled to disclose or provide access to any Company Personal Data to law enforcement or a third party or becomes aware of direct access by law enforcement authorities, Vendor shall notify Company of such action unless prohibited by law.

10.2. Vendor shall not provide any third party: (i) direct, indirect, blanket or unfettered access to Company Personal Data; (ii) encryption keys used to secure Company Personal Data or the ability to break such encryption; or (iii) access to Company Personal Data if Vendor is aware that the data is to be used for purposes other than those stated in the third party's request.

11. **Deletion or Return of Company Personal Data**.

11.1. Following termination or expiration of this DPA, or upon written request of Company, Vendor shall, at the choice of Company, securely destroy Company Personal Data or return Company Personal Data to Company and destroy existing copies, unless applicable law requires retention of Company Personal Data. If Vendor is required to retain Company Personal Data to comply with applicable law, Vendor must inform Company of such legal requirement. Vendor shall continue to comply with this DPA with respect to such retained Company Personal Data and only Process such data to the extent and for so long as required by applicable law.

11.2. Any Company Personal Data returned to Company shall be returned in a commonly used, structured, electronic, and machine-readable format or in such format as otherwise reasonably requested by Company.

11.3. Immediately after destroying Company Personal Data, Vendor shall provide to Company certified written confirmation of such secure destruction.

12. **Recordkeeping**. Vendor shall maintain a record of all Processing activities carried out on Company's behalf in accordance with Data Protection Laws. Vendor shall make such record available to Company and the applicable Supervisory Authority upon request.

13. **Data Protection Impact Assessments**. To the extent required by Data Protection Laws, Vendor shall provide all reasonable assistance to Company to ensure Company is compliant with its obligations under Data Protection Laws related to conducting data protection impact assessments and privacy impact assessments and seeking prior consultation or approval from Supervisory Authorities.

14. **Cooperation.** Vendor shall inform Company immediately if it receives a request from a Supervisory Authority or other governmental authority related to the Processing of Company Personal Data, which Company may decide to resolve at its sole discretion. Vendor shall cooperate with Company to respond to requests from Supervisory Authorities or other governmental authorities that relate to the Processing of Company Personal Data by Vendor or Subprocessors.

15. **Claims.** If Company faces an actual or potential claim arising out of or related to an alleged violation of any Data Protection Laws, Vendor shall promptly provide all materials and information requested by Company that are relevant to the defense of such claim and the underlying circumstances concerning the claim.

16. **Insurance**. In addition to any other insurance required under the Agreement, Vendor shall maintain insurance coverage for privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to Personal Data Breaches, and legal claims for Personal Data Breaches, privacy violations, and notification costs) of at least $3,000,000.00 U.S. per occurrence.

17. **Allocation of Costs**. Each Party shall perform its obligations under this DPA at its own cost, unless otherwise specified herein.

18. **Noncompliance; Remedies**.

18.1. If Vendor can no longer meet its obligations under this DPA, including its obligations under the Standard Contractual Clauses (if applicable), it shall immediately stop Processing Company Personal Data (other than merely storing and maintaining the security of the affected Company Personal Data) and notify Company by email at dataprivacy@dieboldnixdorf.com. Vendor will cooperate with Company's instructions regarding any unauthorized Processing of Company Personal Data by Vendor.

18.2. Any breach of any provision of this DPA may result in irreparable harm to Company, for which monetary damages may not provide a sufficient remedy, and therefore, Company may seek both monetary damages and equitable relief. In the event Vendor breaches any of its obligations under this DPA, Company will have the right to suspend Vendor's continued Processing of any Personal Data, without penalty, immediately upon notice to Vendor.

19. **Termination**. Any material breach of this DPA by Vendor shall constitute a material breach of the Agreement that:

21.1 Gives rise to Company's termination rights under the Agreement; and

21.2 Shall not be subject to any limitation or exclusion of liability provisions contained in the Agreement.

20. **Indemnity**. Vendor shall indemnify, defend and hold harmless Company, its affiliates, officers, directors and employees against all claims, actions, losses, external claims, demands, liabilities, suits, enforcement actions, damages, penalties, fines, expenses and costs (including attorneys' fees, consultants' fees and court costs) arising from or related to (i) the failure of the Vendor to comply with Data Protection Laws; (ii) any breach of this DPA; (iii) any Personal Data Breach; (iv) the negligence, gross negligence, bad faith or intentional or willful misconduct of Vendor or Vendor personnel in connection with the obligations set forth in this DPA; (v) Vendor's failure to anonymize and/or de-identify personal data in accordance with the Agreement; and (vi) Vendor's use of a Subprocessor and/or the Subprocessor's acts or omissions in relation to Company Personal Data.

21. **Amendment**. This DPA may be amended upon written agreement by both Parties. If changes to Data Protection Laws require this DPA to be amended, the Parties will work in good faith to amend the DPA.

22. **Third-Party Beneficiaries**. Company's subsidiaries and affiliates are intended third-party beneficiaries of this DPA and this DPA is intended to relay the same benefits to Company's subsidiaries and affiliates.

23. **Processing of Personnel Personal Data**. In some cases, Company may Process Personal Data of Personnel (i.e., name, business email address, phone number). Details related to this Processing are provided in Company's privacy notice available at: https://www.dieboldnixdorf.com/en-us/privacy-policy/global-privacy-notice..

IN WITNESS WHEREOF, Company and Vendor have executed this DPA as of the Effective Date.

Diebold Nixdorf	[VENDOR]
_____	_____
Authorized Signatory	Authorized Signatory
_____	_____
Name	Name
_____	_____
Title	Title

ANNEX 1: DESCRIPTION OF PROCESSING

Subject Matter of Processing: The subject matter of the Processing is [ ].

Nature and Purpose of Processing: The nature and purpose of the Processing is [ ]

Duration of Processing: The duration of the Processing is the term of the Agreement and until all Company Personal Data has been destroyed or returned in accordance with Section 11 of this DPA.

Categories of Company Personal Data: Vendor Processes the following categories of Company Personal Data: [ ]

Types of Data Subjects: Vendor Processes Company Personal Data of the following types of Data Subjects: [ ]

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Supplier shall at all times comply with the requirements set forth in these SUPPLIER SECURITY REQUIREMENTS ("**Security Requirements**"). These Security Requirements are deemed a part of and incorporated into the Master Services Agreement to which these Security Requirements are attached or incorporated (the "**Agreement**"). The provisions set forth in these Security Requirements shall control in the event of a conflict between the terms and conditions of the Agreement (including any other schedules, exhibits or attachments to the Agreement) and these Security Requirements. Capitalized terms not defined in these Security Requirements shall have the meanings ascribed to them in the Agreement.

DEFINITIONS

a. "**Confidential Information**" has the meaning attributed to it in the Agreement and shall also include: (i) all data, formulae, processes, Cardholder Data (as defined in PCI DSS), procedures, procurement strategies and practices, fees, purchasing volumes, documentation, conclusions, analysis, information, Personal Data, records, specifications, evaluations, know how, business, assets, products, processes, and prospects related to DN communicated to, supplied to, or observed by Supplier, directly or indirectly, at any time, (ii) information related to usage of the Supplier Environment, reports and any data gathered, created or compiled by Supplier as a part of or in connection with the Services hereunder, and (iii) any other information that Supplier should reasonably understand to be considered Confidential Information whether or not such information is marked "Confidential" or contains such similar legend at the time of disclosure. For the purposes of the Security Requirements, any reference to "Confidential Information" shall mean "DN Confidential Information".

b. "**DN Environment**" means any and all facilities, equipment, workstations, servers, cloud environments, software, mobile devices, networks, storage devices, applications, and other systems owned and managed by DN.

c. "**Industry Standards**" means the most current version of the following industry standards, as may be updated or replaced from time to time, reasonably selecting between NIST and ISO standards, which include:

- ISO 27001 – Security techniques – Information security management systems – Requirements.
- ISO 27002 – Security techniques — Code of practice for information security controls.
- NIST Cyber Security Framework and applicable controls NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations.
- NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations.
- NIST Special Publication 800-190 Application Container Security Guide.
- CIS—Center for Internet Security.
- if Confidential Information is Processed or stored in a public cloud, compliance with a "moderate" impact security level in accordance with FedRAMP.
- CSA - Cloud Controls Matrix version 4.
- PCI DSS.
- PA DSS.
- NIST Special Publication 800-88 - Guidelines for Media Sanitization.
- NIST Special Publication 800-61 - Computer Security Incident Handling Guide.
- NIST Special Publication 800-37 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

d. "**Personnel**" means the employees of Supplier and its subcontractors, including permanent employees, fixed-term contract employees, and temporary workers.

e. "**Supplier Environment**" means any and all Supplier or subcontractor facilities, equipment, workstations, servers, cloud environments, software, mobile devices, networks, storage devices, applications, and other systems that Process Confidential Information, or that provide or are used in connection with providing the Services to DN.

2 SECURITY PROGRAM AND RISK MANAGEMENT

Information Security Program. Supplier shall, on a continuous basis while storing or otherwise Processing Confidential Information, develop, implement, maintain, monitor, and as necessary improve and update a comprehensive, written information security program applicable to the protection of the security, confidentiality, integrity, and availability of Confidential Information (the "**WISP**"). Such WISP shall be reasonably consistent with Industry Standards, best practices, and applicable law, and shall contain administrative, technical, and physical

safeguards necessary to protect and ensure the security, confidentiality, integrity, and availability of the Supplier Environment and Confidential Information. The WISP must include a documented plan for incident prevention, detection, and response in accordance with Industry Standards and applicable law, which is reviewed at least annually.

Point of Contact. Supplier shall identify a single point of contact for all communications regarding information security who shall: (i) serve as DN's primary security contact, (ii) have an appropriate level of industry security training and experience, and (iii) be available to assist DN twenty-four (24) hours per day, seven (7) days per week in the event of a Security Breach.

Supplier Personnel Training. Supplier shall ensure that Personnel who will have access to DN's Confidential Information, DN Environment and the Supplier Environment are regularly trained on how to comply with Supplier's WISP and the terms of these Security Requirements. Only Supplier Personnel with a business need in connection with the Services provided during the course of the Agreement may have access to Confidential Information. Supplier's WISP shall take into account whether and how Personnel should be allowed to use or otherwise Process records containing Confidential Information inside and outside of business premises. Supplier will impose disciplinary measures for violations of the WISP and these Security Requirements by its Personnel.

DN Provided Training. Supplier acknowledges that any of its Personnel who have access to the DN Environment shall be required to attend DN security training as determined by DN from time to time. Supplier shall ensure that its Personnel complete such required training.

Risk Assessment. Supplier shall conduct regular (at least annually) assessment of the internal and external risks to the security, confidentiality, integrity, and availability of Confidential Information and the Supplier Environment ("**Risk Assessments**"). Risk Assessments shall be conducted following Industry Standards and best practices, and, without limiting the foregoing, shall at least include vulnerability scanning, penetration testing, social engineering tests, infrastructure design assessments, and data communication assessments.

Risk Management. Supplier shall ensure that Supplier's WISP, the Supplier Environment, and the Services are: (i) designed, maintained, updated, and adjusted, as necessary and at Supplier's sole cost and expense, to adequately control and mitigate the risks identified through Supplier's Risk Assessment, and (ii) regularly tested and monitored to ensure the effectiveness of the key controls, safeguards, systems, and procedures.

SUPPLIER ADMINISTRATION AND EMPLOYEES

Security Administration. Supplier shall manage administrative controls over its compliance with these Security Requirements.

Security Administrators. In accordance with Industry Standards, Supplier must take appropriate actions to prevent unauthorized access to and use of the Supplier Environment and Confidential Information. Supplier management Personnel must retain sole responsibility for granting access to the Supplier Environment for all Personnel.

Personnel Access. Personnel access must be given following the "least privileged principle" and access must be modified upon the change of job function, transfer, or termination of any Personnel who has access to the Supplier Environment or Confidential Information. Supplier must limit Personnel access to the Supplier Environment for the purpose of making maintenance changes to only those Personnel who require access by their job responsibilities and in accordance with the least privileged principle.

Supplier Personnel. Supplier must require its Personnel to report suspected violations of Supplier's security policies (including the WISP) to Supplier management for investigation and action. Supplier must implement and document consequence management policies for violations of Supplier's security policies (including the WISP).

CONTROLS AND REQUIREMENTS

Controls and Requirements. Supplier shall implement and maintain such controls, processes, technology, training, and procedures as is necessary to protect the security, confidentiality, integrity, and availability of Confidential Information and the Supplier Environment. Without limiting the generality of the foregoing, and except where Industry

Standards or applicable law require more protective measures, Supplier shall at least comply with the more particular requirements that follow in this Section 4.

Encryption. Supplier shall encrypt all Confidential Information in transit and at rest, in accordance with Industry Standards, and must be at least FIPS 140-2. Any exceptions must be previously agreed by DN in writing. Passwords stored in databases must be one-way hashed and otherwise meet Industry Standards and best practices. All Confidential Information stored in Supplier repositories or otherwise backed up must be encrypted prior to backup.

Logs. Supplier shall log, in accordance with Industry Standards and best practices, all activities by its Personnel and others related to accessing the Supplier Environment and Processing Confidential Information. Logs must be retained for a minimum of two (2) years. Supplier shall maintain log management operational processes consistent with Industry Standards and best practices. Logging must at a minimum include the following: date and time of each logged event; when session ends; source and destination IP address; user ID; details of attempted, successful and rejected access attempts; type of activity performed; and modifications. Supplier must maintain such logs in accordance with applicable law and these Security Requirements.

Data Security Controls. Supplier must document, implement, maintain, and update adequate data security controls in Supplier Environment, such as, but not limited to, logical access controls including user sign-on identification and authentication, data access controls (e.g., password protection of Supplier Environment, data files, databases, repositories, and libraries), accountability tracking, anti-virus software, secured printers, and restricted download to disk capability.

Systems Security. Supplier shall establish and maintain a security system covering the Supplier Environment, including any wireless systems, that, at a minimum, shall have the following elements:

Secure user authentication protocols including: (i) control of user IDs and other identifiers, (ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices, (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect, (iv) restricting access to active users and active user accounts only, and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or other limitations placed on access for the particular system.

Secure access control measures that: (i) restrict access to records and files containing Confidential Information to those who need such information to perform their job duties, and (ii) assign unique identifications plus passwords, which are not Supplier supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

Networks in the Supplier Environment must be configured so that each desktop and all inbound and outbound mail servers have current anti-virus protection. The Supplier Environment shall include up-to-date versions of system security agent software which must include malware protection and up-to-date patches and virus definitions (all of which must be set to receive the most current security updates on a regular basis). For files containing Confidential Information on the Supplier Environment, there must be up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of Confidential Information.

Supplier shall use commercially reasonable efforts to log, monitor, and prevent the installation, spread, and execution of malicious software in the Supplier Environment, and take immediate defensive and corrective actions in accordance with Industry Standards and best practice.

Patching. Supplier shall implement and maintain a patch management program that covers the Supplier Environment and that follows Industry Standards and best practices. Supplier shall scan the Supplier Environment for and remediate vulnerabilities on a continuous basis in a timeframe commensurate with the severity of the vulnerability, not to exceed the following timeframes:

- Critical vulnerabilities (CVSS Score 9.0+ or the equivalent) = 30 days
- High vulnerabilities (CVSS Score 7.0-8.9 or the equivalent) = 30 days
- Medium vulnerabilities (CVSS Score 4.0-6.9 or the equivalent) = 90 days
- Low vulnerabilities (CVSS Score < 4.0 or the equivalent) = 180 days

Where for good cause (e.g., because the patch failed testing) a patch cannot be timely implemented, Supplier shall implement effective compensating and mitigating controls.

Supplier Network. All access to the Supplier Environment shall require multi factor authentication, including a user ID and password or an equivalent security credential. Supplier must ensure that user IDs and passwords for the Supplier Environment are controlled as follows: (i) unique ("single user") ownership of user ID, (ii) no "generic" or group user ID, (iii) immediate revocation or deletion of all access rights for any terminated, leave of absence, or transferred Personnel, (iv) access rights to Confidential Information shall be provided on a "need to know", job function basis, (v) if a user ID is revoked, re-authentication and positive identification of the user must occur before the user ID can be reactivated, and (vi) passwords must meet Industry Standards or regulatory standards, as applicable. User IDs must be locked after no more than five (5) failed log-in attempts and must remain locked until the system administrator for the system resets the user's account, or until the allotted time to automatically reset login attempts has passed which shall be at least ten (10) minutes.

System and Network Security. Supplier must document and maintain adequate network-based and end point intrusion detection capabilities and intrusion prevention capabilities.

Backups and Disaster Recovery. Supplier shall regularly maintain secure backups of the Supplier Environment, including any Confidential Information, sufficient to recover the Services and the Supplier Environment from events that affect the security, integrity, or availability of Confidential Information and the correct and sufficient provision of the Services. Supplier shall maintain business continuity and disaster recovery plans, and the means to successfully execute such plans, to meet its requirements herein. Supplier shall carry out annual tests to ensure its backup and disaster recovery plans meet these requirements.

Changes to Security. Supplier shall notify DN of any technical or policy change that may materially decrease the level of security in the Supplier Environment or that may cause the Supplier to not be in compliance with these Security Requirements. Supplier shall notify DN at least 30 days prior to such changes being implemented.

5 PHYSICAL SECURITY CONTROLS

Sites. Supplier must document, implement, maintain, and update adequate physical security controls over all facilities hosting the Supplier Environment and where Confidential Information is Processed (collectively, "**Sites**"). Without limiting the foregoing, Supplier shall implement and maintain reasonable restrictions upon physical access to Confidential Information, including a written procedure that sets forth the manner in which physical access to such records is restricted. Storage of records and data must be done in locked facilities, storage areas, and containers. Supplier shall implement at the Sites security and environmental controls over all computer rooms and equipment that will be used in conjunction with Confidential Information and the Services, including restricting access to only approved staff.

Secure Disposal. Supplier shall implement at the Sites secure disposal programs that provide for the secure disposal and destruction of all storage media (e.g., data tapes, hard drives and other storage media containing Confidential Information) and any discarded material (including electronic media) that contains or could disclose Confidential Information. Such programs must be implemented in accordance with Industry Standards.

DN ENVIRONMENT

Access to the DN Environment. Supplier may only access the DN Environment from a Supplier authorized service location for the purpose of performing the Services under the Agreement. Supplier will not allow access to the DN Environment to any third parties without prior written consent from DN. Any such access is subject to additional policies, controls, and requirements provided by DN from time to time. All access to the DN Environment shall be via a DN approved secured connection.

Workstations. Supplier must ensure all workstations which allow access to Confidential Information and the DN Environment or which are used to provide the Services are controlled and protected in accordance with these Security Requirements, including, without limitation, required firewalls, antivirus software, intrusion detection, and endpoint detection and response applications. All such workstations must be: (i) equipped with appropriate access control, including password protected screen savers, and time-out after 15 minutes or less of non-use, and (ii) configured such that they do not enable or facilitate the transfer of Confidential Information by any portable storage medium (e.g., Zip Drives, USB memory devices, etc.), by email, or by other means such that Personnel could distribute Confidential Information without permission or consent by DN or as permitted under the Agreement. Workstations must be

configured so that Personnel cannot download or install software from any source other than those expressly approved by Supplier. Persistent local administrator permissions are prohibited.

User access. Upon request, Supplier shall provide an updated list of all accounts, users, profiles, or similar access credentials which have access to the DN Environment.

SECURITY INCIDENTS

Security Breaches. In the event Supplier becomes aware of any actual or reasonably suspected unauthorized access to or use, disclosure, alteration, loss or destruction of Confidential Information and/or the Supplier Environment ("**Security Breach**"), Supplier shall, within twenty-four hours after becoming aware of a Security Breach, notify DN of such Security Breach via email to InformationSecurity@dieboldnixdorf.com, specifying the details of the Security Breach and what Confidential Information has been impacted. For the avoidance of doubt, ransomware attacks affecting Confidential Information, or the Supplier Environment are considered Security Breaches.

Response. Supplier shall: (i) immediately take action to contain such Security Breach and mitigate potential risks to Confidential Information and the Supplier Environment, and the DN Environment (to the extent impacted), (ii) investigate the Security Breach (including determining what systems, data, and information have been affected by the Security Breach) and perform a root cause analysis thereon, (iii) report its findings to DN on a continuous basis (at least daily) until the investigation is completed, as reasonably determined by agreement of the Parties, (iv) provide DN with a remediation plan to address the Security Breach and prevent any further incidents, (v) remediate the Security Breach, (vi) cooperate with DN and, at DN's request, any law enforcement or regulatory officials investigating such Security Breach, and (vi) provide all reasonably requested evidence and information in relation to the Security Breach (i.e.: logs, reports, etc.).

Notification. Except where required by applicable law, (i) Supplier shall not notify any third party (including any individual or government authority) of any Security Breach without first obtaining DN's prior written consent, and (ii) DN shall have the sole right to determine the contents of any such notice of a Security Breach to the extent that it may be associated with or linked to DN.

Reimbursement. Supplier shall indemnify and reimburse DN for all Security Breach Related Costs (defined below) incurred_by DN arising out of or in connection with a Security Breach. Such indemnification and reimbursement obligation is not capped or limited by the Agreement, including any limitation on liability therein. "Security Breach Related Costs" means any costs associated with addressing and responding to a Security Breach, including, but not limited to: (i) preparation and mailing or other transmission of notifications to impacted individuals and/or governmental authorities; (ii) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (iii) public relations and other similar crisis management services; and (iv) legal, forensic and accounting fees and expenses associated with DN's investigation of and response to such Security Breach.

AUDITS AND VERIFICATION

Operational Audits. Once a year, or whenever there is a Security Breach, a breach of these Security Requirements, or as requested by a regulator, Supplier shall give DN and its auditors (including internal audit staff and external auditors) access at all reasonable times to the Supplier Environment, Confidential Information, and any Supplier facility relating to the Services, for the purpose of performing audits of either Supplier or any of its subcontractors to verify whether the Supplier's or its subcontractors' security practices comply with applicable law and these Security Requirements. Supplier shall make appropriate Personnel available to facilitate the audit process.

Security Questionnaires. Supplier shall complete and return any information security survey, information request or questionnaire provided by DN within 10 business days after receipt.

Third Party Audits. At DN's request, and for no additional compensation, Supplier shall provide its SSAE 18 SOC 1, SOC 2 Type II, and ISO 27001 (or their successor standards) audit of controls report applicable to the Services and related Supplier Environment.

Documentation. Supplier must, upon DN's request, provide to DN: (i) copies of all internal security policies, network architecture/diagrams in relation to the Services, and standards for DN's review, and (ii) a copy of the most recent internal and/or third-party data processing or security audit or review reports, including any recent risk or security assessments, reports on compliance, penetration tests, vulnerability scans, and controls assessments, that may apply.

Access to reports. DN shall have the right to provide all reports, opinions and certifications delivered hereunder to its employees and professional advisors who shall have obligations of confidentiality regarding such information and only on a need-to-know basis. DN may provide such reports, opinions, and certifications to a government regulator.

Monitoring. DN reserves the right to monitor access and use of the DN Environment in any manner determined by DN.

OTHER SECURITY REQUIREMENTS

Secure Software Standards. Supplier represents and warrants any software developed as part of or in connection with the Services will be securely developed and maintained throughout the software development life cycle following Industry Standard secure coding processes, practices, training, testing, and controls. Supplier must ensure that software code delivered to DN as part of the Services complies and was developed in accordance with Industry Standards and best practices (e.g., OWASP), is free from security vulnerabilities, and, if applicable, does not prohibit DN from obtaining their annual PCI DSS compliance or meeting similar government or regulatory requirements needed to maintain their normal course of business. Supplier agrees to the escrow of all proprietary source code used in performance of the Agreement with a mutually agreeable third party, identifying DN as beneficiary.

Development Separation. Supplier shall maintain procedures to physically and/or logically separate any application development and production servers and environments. Live data, including direct copies of production Confidential Information, shall not be used in any non-production environment, including development and test systems Development staff must not have access to the production servers and operations staff must not generally have access to the development source.

PCI. The provisions set forth in this Section apply to Supplier if, either by itself or through a processor or other agent, Supplier stores, processes or transmits Cardholder Data (as defined in the PCI SSC) in any manner, or if, in relation to the Services, Supplier otherwise could impact the security of DN's Cardholder Data environment. Where any of the above conditions apply, Supplier is and shall be in compliance with applicable Payment Card Industry Data Security Standards (**"PCI DSS"**) requirements, as set forth in the current version of PCI DSS and any amendments or modifications thereto or new versions made effective in the future. The Parties will agree in writing to any specific requirements necessary for the provision of the Services. To validate such compliance, Supplier will either: (i) undergo a PCI DSS assessment and provide evidence to DN to demonstrate such compliance, or (ii) permit its services and/or environments, as applicable, to be reviewed during the course of any DN PCI DSS assessment.

Payment Card Industry Requirements. In performing the Services, Supplier shall adhere to all Payment Card Industry Standards as applicable to Supplier's provision of the Services. Supplier shall provide to Diebold Nixdorf all documents reasonably requested by Diebold Nixdorf to show compliance, including a "Report of Compliance" from a Qualified Security Assessor. The cost to obtain such "Report of Compliance" shall be borne by the Supplier and in no event shall Diebold Nixdorf be obligated to pay costs in connection with Supplier obtaining such "Report of Compliance".

MISCELLANEOUS

Subcontractors. Supplier shall ensure and verify that its agents, suppliers, and subcontractors comply with these Security Requirements and applicable law.

10.2 **Conflict with Law.** Where applicable law prevents compliance with the Security Requirements, Supplier shall notify DN of such applicable laws in order to determine appropriate compensating controls. Where applicable law sets forth more stringent requirements than those set forth in these Security Requirements, Supplier shall comply with applicable law

ANNEX 3: LOCATION OF PROCESSING

1. Name:
   Address:

ANNEX 4: STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

1. For purposes of the Controller-to-Processor Standard Contractual Clauses (Module 2), Company is the "data exporter" and Vendor is the "data importer." The Parties agree to the following terms:

   a. Incorporation by Reference. The Parties shall abide by and transfer Company Personal Data in accordance with the Controller-to-Process Standard Contractual Terms (Module 2), which are incorporated into this DPA by reference. Each Party is deemed to have executed the Standard Contractual Clauses by executing this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses is set out in Annex 2 (technical and organizational measures) and Annex 5 (description of processing).

   b. Docking Clause. The option under Clause 7 of the Standard Contractual Clauses shall not apply.

   c. Onward Transfers. For the purposes of Clause 8.8 of the Standard Contractual Clauses, Vendor is responsible for executing Standard Contractual Clauses with any third party or ensuring third party's compliance with the requirements set out in Clause 8.8 of the Standard Contractual Clauses.

   d. Authorization of Subprocessors. For the purposes of Clause 9 of the Standard Contractual Clauses, Option 1 (Specific Prior Authorisation) is selected and the process and time period for Subprocessors shall be as described in Section 5 of this DPA.

   e. Subprocessors and Onward Transfers. For the purposes of Clause 9(b) of the Standard Contractual Clauses, Vendor must require that a Subprocessor enter into Standard Contractual Clauses if it engages its own Subprocessor to Process Company Personal Data in a Third Country.

   f. Supervisory Authority. Clause 13(a) of the Standard Contractual Clauses shall apply as follows:

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

   g. Government Access Requests. For the purposes of Clause 15(1)(a) of the Standard Contractual Clauses, Vendor shall notify Company (only) and not the Data Subject(s) in case of government access requests.

   h. Governing Law and Jurisdiction. For the purposes of Clause 17 and Clause 18 of the Standard Contractual Clauses, the Member State for purposes of governing law and jurisdiction shall be Germany.

2. In case of any transfers of Company Personal Data from the United Kingdom and/or transfers of Company Personal Data from Switzerland subject exclusively to the Swiss Data Protection Law, (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or EEA Member State law shall have the same meaning as the equivalent reference in UK Data Protection Laws or Swiss Data Protection Law, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the EEA Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Law, as applicable. In respect of data transfers governed by Swiss Data Protection Law, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Company Personal Data under Swiss Data Protection Law until such laws are amended to no longer apply to a legal entity.

ANNEX 5: DESCRIPTION OF PROCESSING/TRANSFER

1. LIST OF PARTIES

Data exporter(s):

Name: _____

Address: _____

Contact person's name, position and contact details: _____

dataprivacy@dieboldnixdorf.com_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): Controller

Data importer(s):

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): Processor

2. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

[ ]

Categories of personal data transferred

[ ]

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation,

access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

[ ]

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

[ ]

Nature of the processing

[ ]

Purpose(s) of the data transfer and further processing

[ ]

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

The duration of the Processing is the term of the [ ] and until all personal data processed by data importer on behalf of data exporter has been destroyed or returned in accordance with the data processing agreement.

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

[ ]

3. COMPETENT SUPERVISORY AUTHORITY

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

Germany

4. LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): …

