

[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 includes 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 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

1. **Sharing Personal Data with Third Parties** – Add Section [X] to Data Processing Documents as follows:

Section [X] Sharing Controller personal data with third parties.

Processor shall not disclose or provide access to any personal data to law enforcement or any other third party unless required by law. If Processor is contacted with a demand for personal data, Processor shall (i) attempt to redirect the law enforcement agency or other third party to request the personal data directly from Controller, (ii) reject the request or demand unless required by law to comply, and (iii) promptly notify Controller and provide Controller a copy of the request or demand unless legally prohibited from doing so. If Processor is compelled to disclose or provide access to any personal data to law enforcement or a third party or becomes aware of direct access by law enforcement authorities, Processor shall notify Controller of such action unless prohibited by law.

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

2. **Technical and Organizational Measures** – Add to Section [X] of Data Processing Documents the following provision:

Processor shall 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 personal data; Such measures are specific in Annex [8] to the Data Processing Documents.

3. **Transfers** - Add Section [X] to Data Processing Documents as follows:

Section [X] Data transfers

OPTION 1:

[The Parties acknowledge that neither Vendor nor any Subprocessor 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:

Processor shall not transfer, or cause to be transferred, personal data from one country to another without Controller's prior written consent. Where Controller consents to such transfer, the transfer shall be in accordance with data protection laws. Processor shall at all times provide an adequate level of protection for personal data wherever processed in accordance with data protection laws.

Annex [4] lists the locations where personal data will be processed by Processor and any subprocessors. The Parties shall enter into and comply with:

- a. the Controller-to-Processor Standard Contractual Clauses (Module 2), subject to the additional terms in Annex [5] for the transfer of personal data from the European Economic Area ("EEA") and/or Switzerland to any Third Country.
- b. the provisions of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for the transfer of personal data from the United Kingdom ("UK") to any Third Country (the "UK Addendum") in accordance with the terms of Annex [7].

If Processor has implemented binding corporate rules, Processor's binding corporate rules shall apply to the transfer of personal data to a Third Country and the Standard Contractual Clauses and/or UK Addendum shall not apply. Processor shall also enter into Standard Contractual Clauses and/or UK Addendum, or rely on subprocessor's binding corporate rules, for onward transfers of personal data to subprocessors processing personal data in Third Countries.

Processor shall assist Controller with completing any assessments for transfers of personal data outside of the EEA, UK and/or Switzerland, including by providing any information reasonably requested by Controller related to a subprocessor. The Parties shall work together to implement safeguards that Controller deems necessary to ensure transfers of personal data to Third Countries comply with data protection laws.

If any of the data transfer mechanisms set forth in this section of this agreement 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 personal data that comply with data protection laws.

For the purposes of this agreement, the terms listed below shall be defined as follows:

“**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.

“**Third Country**” means (i) with respect to personal data of data subjects in the EEA, any country, organization or territory not acknowledged by the European Union under Article 45 of the GDPR as a safe country with an adequate level of data protection; and (ii) with respect to personal data of data subjects in the UK, any country, organization or territory not acknowledged by the UK Parliament under the UK data protection laws as a safe country with an adequate level of data protection.

4. **Audit** – Add Section to Data Processing Documents as follows:

Section Audit and inspections

Upon request, but no more than once a calendar year (unless in relation to a personal data breach or a request from a regulator), Processor shall make available to Controller any information Controller may require (including information about subprocessors) for purposes of demonstrating compliance with Controller’s obligations under this agreement. Upon request, Processor shall supply Controller with a copy of its most recent internal or third-party audits and/or certifications pertaining to security, availability, processing integrity, confidentiality, and privacy.

Processor shall allow for and contribute to audits conducted by Controller or another auditor instructed by Controller that is not a competitor of Processor, subject to confidentiality requirements similar to those applicable to Controller. Controller will bear the cost of the audit. Processor will bear the costs of remediation for any material gaps found during the audit. If requested by a regulator, Processor authorizes Controller to share with such regulator (i) any information Processor provides pursuant to this agreement, and (ii) the results of any audit Controller conducts pursuant to this agreement.

5. **Breach** – Add Section of Data Processing Documents as follows:

Section Personal data breach.

Processor shall without undue delay, and at the latest, within 24 hours after becoming aware of a personal data breach, notify Controller 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, Processor may provide such information to Controller in a phased manner as the information becomes available.

Processor shall immediately take action to contain such personal data breach and mitigate potential risks to affected data subjects. Processor shall keep Controller advised of the status of the personal data breach.

Processor shall provide all assistance and cooperation reasonably requested by Controller, in furtherance of (i) any correction, remediation or investigation of a personal data breach and/or the mitigation of any damage, and (ii) any action Controller 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.

Processor 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 Controller, or where required by law.

For the purposes of this agreement, a “**personal data breach**” means any actual or reasonably suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data or breach of security of Processor’s or its subprocessors’ systems processing personal data.

6. **Location of Processing** - Add Annex [X] to Data Processing Documents as follows:

ANNEX [X]: LOCATION OF PROCESSING

1. **Name:**
Address:

7. **Standard Contractual Clauses**

- a. Add Annex [X] to Data Processing Documents as follows:

ANNEX [X]: STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

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

1. Incorporation by Reference. The Parties shall abide by and transfer personal data in accordance with the Controller-to-Processor Standard Contractual Clauses (Module 2), which are incorporated into this agreement by reference. Each Party is deemed to have executed the Standard Contractual Clauses by executing this agreement. The information required for the purposes of the Appendix to the Standard Contractual Clauses is set out in Annex [X] to the Agreement (Description of Processing) and Annex [X] DN Supplier Security Requirements.
2. Docking Clause. The option under Clause 7 of the Standard Contractual Clauses shall not apply.
3. Onward Transfers. For the purpose of Clause 8.8 of the Standard Contractual Clauses, Processor 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.
4. Authorization of Subprocessors. For the purpose of Clause 9 of the Standard Contractual Clauses, Option 1 (Specific Prior Authorisation) is selected. Processor shall submit the request for specific authorization to Controller (by email to dataprivacy@dieboldnixdorf.com) at least one month in advance of its engagement of a new subprocessor.
5. Subprocessors and Onward Transfers. For the purpose of Clause 9(b) of the Standard Contractual Clauses, Processor must require that a subprocessor enter into Standard Contractual Clauses if it engages its own subprocessor to process personal data in a Third Country.
6. 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.
7. Government Access Requests. For the purposes of Clause 15(1)(a) of the Standard Contractual Clauses, Processor shall notify Controller (only) and not the data subject(s) in case of government access requests.

8. 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.
9. In case of any transfers of personal data from Switzerland subject exclusively to Swiss data protection law, (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or EEA Member State law shall include Switzerland and have the same meaning as the equivalent reference in Swiss data protection law, as applicable; (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 Swiss data protection law, as applicable; and (iii) the Federal Data Protection and Information Commissioner is the competent supervisory authority. 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 personal data under Swiss data protection law until such laws are amended to no longer apply to a legal entity.
- b. Add Annex to Data Processing Documents as follows:

ANNEX : DESCRIPTION OF PROCESSING/TRANSFER

9. 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

9. 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 6rganizatio training), keeping a record of access to the data, restrictions on 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 agreement.

9. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: [] COMPETENT SUPERVISORY AUTHORITY

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

Germany

4. LIST OF SUB-PROCESSORS

The controller has organized 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):

8. **International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**
Add Annex [7] to Data Processing Documents as follows:

ANNEX [X]: INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

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

Part 1: Tables

Table 1: Parties

Start date	Effective Date of Amendment	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: See Annex 6 Trading name (if different): [] Main address (if a company registered address): See Annex 6 Official registration number (if any) (company number or similar identifier):	Full legal name: See Annex 6 Trading name (if different): [] Main address (if a company registered address): See Annex 6 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): See Annex 6 Job Title: See Annex 6	Full Name (optional): See Annex 6 Job Title: See Annex 6

	Contact details including email: See Annex 6	Contact details including email: See Annex 6
Signature (if required for the purposes of Section 2)	See Annex 6	See Annex 6

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: <input type="text"/> Reference (if any): <input type="text"/> Other identifier (if any): <input type="text"/> Or <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:
-------------------------	--

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	x	No	N/A	<input checked="" type="checkbox"/> Prior authorization <input type="checkbox"/> General authorization	10 business days	N/A
	x	No	N/A	<input checked="" type="checkbox"/> Prior authorization <input type="checkbox"/> General authorization	10 business days	N/A

Table 3: Appendix Information

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

Annex 1A: List of Parties: See Annex 6
Annex 1B: Description of Transfer: See Annex 6
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: See Annex 3 to the Agreement.
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex 6

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p><input type="checkbox"/> Importer</p> <p><input checked="" type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
--	---

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

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

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

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

Hierarchy

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

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

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

Incorporation of and changes to the EU SCCs

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

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

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

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

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

- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
- c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
- d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
- f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
- i. The reference to "Clause 11)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
- l. In Clause 16(e), subsection (i) is replaced with:

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

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

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

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

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

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

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

9. Technical and Organizational Measures / Supplier Security Requirements. Add/Replace Annex [X] to Data Processing Documents as follows:

ANNEX [X]: SUPPLIER SECURITY REQUIREMENTS

The minimum technical and organizational measures to be applied by the Supplier for the provision of the Services are available at: <https://www.dieboldnixdorf.com/-/media/diebold/files/support/data-privacy/dn-supplier-security-requirements-pdf.pdf>