TOSHIBA

Data Processing Agreement

This Data Processing Agreement ("DPA"), shall be effective on the effective date of the Agreement (the "Effective Date"), and entered into by and between Toshiba Global Commerce Solutions ("Toshiba" or "Servicer Provider"), and Customer ("Customer"); each of Servicer and Customer, a "Party", and together, the "Parties"). The Toshiba party to this Agreement is the Toshiba entity that is the Toshiba party to the Agreement. This DPA supersedes any and all other agreements previously entered into by the Parties, or Customer and Toshiba, pertaining to the subject matter contemplated herein.

A. WHEREAS Customer appointed Toshiba to provide the Services in accordance with the terms and conditions set forth in the Master Customer Agreement available on our public webpage https://commerce.toshiba.com/.com (Licenses & Warranties) or the equivalent agreement in place between us ("Agreement");

B. WHEREAS under the Agreement Customer is required to securely erase all personal data or, if removing of personal data is not possible, to transform such information (e.g., by making it anonymous) so that it no longer qualifies as personal data under applicable law;

C. WHEREAS it cannot be excluded that Services to be delivered by Toshiba to Customer under the Agreement nevertheless qualify as processing of Customer's personal data;

D. WHEREAS the Parties therefore desire to amend the Amend to memorialize their mutual obligation, whether as a data controller or data processor, to process or otherwise handle personal data in a way that complies with the applicable Data Protection Legislation; and

E. WHEREAS the Parties therefore wish to include in the Agreement additional provisions related to processing of personal data.

1.1 References in this DPA to "data controller", data processor", "processing", "data protection officer" and "personal data" shall have the same meaning as defined in Data Protection Legislation.

1.2 The parties acknowledge and agree that in order to provide the Services, Service Provider may process personal data. Schedule 1 sets out the subject matter and duration of the processing; nature and purpose of the processing; the type of personal data being processed; and the categories of data subject.

1.3 The parties agree that in respect of any personal data processed in connection with this DPA that Customer shall be the **"data controller"** (as defined in Data Protection Legislation) and Service Provider or Sub Processor shall be the **"data processor"** (as defined in Data Protection Legislation).

1.4 Each party acknowledges and agrees that each party has respective rights and obligations under applicable Data Protection Legislation. Service Provider shall, without prejudice to its other rights or obligations, in respect of its processing of such personal data:

(a) process the data only to the extent, and in such a manner, as is necessary for the purposes of this DPA and in accordance with Customer's lawful written instructions from time to time and Service Provider shall not process, nor permit the processing, of the data for any other purpose unless such processing is required by European Union or a law of a Member State to which Service Provider is subject in which case Service Provider shall notify Customer in advance of its intention to carry out such processing and allow Service Provider the opportunity to object. If Service Provider is unsure as to the parameters of the instructions issued by Customer and/or believes

that Customer's instructions may conflict with the requirements of Data Protection Legislation or other applicable laws, Service Provider may notify Customer for clarification and provide reasonable details in support of any assertion that Customer's instructions may not be lawful;

(b) ensure the reliability of all its personnel who have access to the data and shall in particular ensure that any person authorised to process data in connection with this DPA is subject to a duty of confidentiality;

(c) at Customer's cost take such measures as may be required in line with Article 32 of the GDPR (Security);

(d) at Customer's cost assist Customer by using appropriate technical and organisational measures in responding to, and complying with, data subject requests. At a minimum, these will include the measures set out in Schedule 2;

(e) at Customer's cost, without undue delay notify Customer, and provide such co-operation, assistance and information as Customer may reasonably require if Service Provider:

(i) receives any complaint, notice or communication which relates directly or indirectly to the processing of the personal data under this DPA or to either party's compliance with Data Protection Legislation; and/or

(ii) becomes aware of any Security Breach;

(f) keep at its normal place of business a written record of any processing of the data carried out in the course of the Services ("**Records**");

(g) permit no more than once per year Customer, its third-party representatives (who is not a competitor of Service Provider) or a Regulator, on reasonable notice during normal business hours, but without notice in case of any reasonably suspected breach of this clause by Service Provider, access to inspect, and take copies of, the Records for the purpose of auditing Service Provider's compliance with its obligations under this clause. Service Provider shall at Customer's cost give all reasonably necessary assistance to the conduct of such audit;

(h) may engage a sub processor to process data (or otherwise sub-contract or outsource the processing of any data to a third party) (a "**Sub processor**"), provided that it:

(i) notifies Customer of any new or replacement Sub processors. If Customer objects to the appointment of a new or replacement Sub processor, it shall notify Service Provider within five business days. Customer shall be deemed to have accepted the Sub processor if Service Provider does not receive an objection with five Business Days. If the objection cannot be resolved by the parties within five Business Days of receipt by the Companies of the written objection, Service Provider shall not be in breach of this DPA to the extent it cannot provide its services or otherwise comply with its obligations as a result;

(ii) enters into a written contract with the Sub processor that:

(1) provides protections or guarantees that Sub processor considers necessary to implement appropriate technical and organisation measures in compliance with the Data Protection Legislation; and

(2) terminates automatically on termination or expiry of this DPA for any reason; and

(iii) remains liable for all acts or omissions of the Sub processors as if they were acts or omissions of Service Provider (except to the extent caused or exacerbated by Customer).

As at the date of this DPA, Service Provider uses the sub-processors, which may include Service Provider's affiliates, set out in Schedule 1 for the activities set out in Schedule 1 in connection with the provision of the Services;

(i) at Customer's cost return or destroy (as directed in writing by Customer) all personal data it has in its possession and delete existing copies unless applicable law requires storage of the personal data.

(j) to the extent that Service Provider is required to transfer personal data pursuant to this DPA to a territory outside of the European Economic Area ("EEA") that does not have a finding of adequacy by the European Commission, the parties shall execute or procure the execution of the standard contractual clauses set out in the 2021 SCCs Module Two and 2021 SCCs Module Three, collectively or individually, as applicable, published under the EU Commission Decision 2021/914/EU ("**Model Clauses**") unless the parties agree another more appropriate lawful data transfer mechanism exists. The parties agree that if the Model Clauses (or agreed alternative mechanism) cease to exist or are no longer considered by both parties to be a lawful method of transferring personal data outside of the EEA, the parties shall have a good faith discussion and agree an alternative lawful transfer mechanism and Service Provider may cease or procure that the relevant third party cease the processing of personal data until such time as the parties have agreed an alternative transfer mechanism to enable the personal data to be transferred outside of the EEA in a compliant manner.

1.5 Customer agrees to comply with its obligations under applicable Data Protection Legislation in respect of the processing of personal data under or in connection this DPA and shall in particular ensure that, as a condition of this DPA, Service Provider is lawfully permitted to process personal data on its behalf. Customer shall indemnify Service Provider on demand against all claims, liabilities, costs, expenses, damages and losses (including all interest, penalties and legal costs and all other professional costs and expenses) suffered or incurred by Service Provider arising out of Customer's breach of this clause 1.5 ("**Claims**"). Each party acknowledges that Claims include any claim or action brought by a data subject arising from the Customer's breach of its obligations in this clause. Service Provider's liability for breach of its obligation in this clause 1 shall in any case be limited to the charges paid in the previous 12 months under the Master Customer DPA. In addition, Service Provider shall not be liable for loss of data.

1.6 For the purpose of this clause 1:

"Data Protection Legislation" means UK Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the UK General Data Protection Regulation and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national Regulators including the UK Information Commissioner;

"**GDPR**" means the EC Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (when in force);

"**Regulator**" means any regulatory body with responsibility for ensuring compliance with Data Protection Legislation.

"**Security Breach**" means accidental or deliberate, unauthorised or unlawful acquisition, destruction, loss, alteration, corruption, access, use or disclosure of personal data processed

under to this DPA or breach of Service Provider's security obligations under this DPA (including clause [1.4](d)).

Schedule 1

Data Processing Services

- the subject matter and duration of the processing: from time to time during the term of the Services under the Master Customer Agreement. Duration of processing and retention period shall be the duration of the Services unless Customer personal data is deleted sooner.
- nature and purpose of the processing: the Service provider may be required to access, receive, generate, store or otherwise process personal data in order to provide IT support and to maintain, improve and develop hardware and software products. Storage and processing of Customer data in cloud and/or support or consulting Services.
- the type of personal data being processed: Customer personal data uploaded to and residing in cloud and/or otherwise processed by Service Provider to provide the Services. Customer personal data may include sensitive personal data as long as such data is not required by an industry specific data law.
- the categories of data subject: Service Provider will not be aware of what personal data the Customer may provide for the Services. It is anticipated that the data subjects may include employees and customers of the Customer.
- location of processing

Location	**Data Transfer Mechanism (if applicable)**
Customer on premise	N/A

- permitted sub-processors and location of processing

Name	**Services**	**Location**	**Data Transfer Mechanism (if applicable)**
Microsoft	Cloud services	EU and UK as selected by the customer	N/A
Arka Service	Support services	Italy	N/A
Bottega52	Application management	Italy	N/A
Spindox	Cloud services	Italy	N/A

- service provider's affiliates

  - *Toshiba Global Commerce Solutions (Benelux) NV, Z.1 Research Park 160, 1731 Zellik, Belgium*
  - *Toshiba Global Commerce Solutions (Denmark) ApS, H. C. Andersens Boulevard 38, 3. th., 1153 København V, Denmark*
  - *Toshiba Global Commerce Solutions (France) SAS, 1-5 rue Eugène et Armand Peugeot, 92500 Rueil-Malmaison, France*

- *Toshiba Global Commerce Solutions (Germany) GmbH, Carl-Schurz-Str. 7, 41460 Neuss, Germany*
- *Toshiba Global Commerce Solutions (Nordic) AB, Frösundaviks Allé 1, 169 70, Solna, Sweden*
- *Toshiba Global Commerce Solutions (Poland) sp. z o.o., ul. Jutrzenki 137 02-231 Warsaw, Poland*
- *Toshiba Global Commerce Solutions (Spain) S.L., Calle Campezo 1, Parque Empresarial Las Mercedes, Edificio 6 – bajo B, 28022 Madrid, Spain*
- *Toshiba Global Commerce Solutions (U.K.) Ltd., 3375 Century Way, Thorpe Park, Leeds LS15 8ZB, England*

TOSHIBA

Schedule 2

Technical and Organizational measure

Klicken Sie hier, um Text einzugeben.

Art. 32 GDPR - Processing Security
(1) With consideration of state-of-the-art technology, implementation costs, and the type, scope, circumstances and purposes of the processing, as well as the different access possibilities and the seriousness of the risk posed to the rights and liberties of natural persons, the responsible employee and the order processor shall decide on suitable technical and organisational measures to guarantee a level of protection appropriate to the risk; these measures include, among other things, the following:

a. the **pseudonymisation** and **encryption** of personal data;
b. permanently ensuring the capacity, the **confidentiality, integrity, accessibility** and **resilience** of the systems and services connected with processing;
c. the fast restoration of capacity, **accessibility** to personal data, and access in the event of a physical or technical incident;
d. a procedure for the regular **testing**, assessment and evaluation **of the effectiveness** of the technical and organisational measures, in order to ensure the security of the processing.

(2) When assessing the appropriate level of protection, the **risks** connected with processing should be taken into account in particular, – especially by **destruction**, **loss** or **modification**, whether unintended or illegal, or the **unauthorised disclosure** of, or **unauthorised access** to personal data which has been transferred, stored or processed in any other manner.

Confidentiality

Access Control

Measures suitable for preventing unauthorised persons accessing the data processing systems in which personal data is processed or used.

☒	Alarm system with a connection to site security	☒	Safeguarding of building shafts
☒	Automatic access control system	☒	Chip card/transponder locking system
☐	Locking system with code lock	☒	Manual locking system
☐	Biometric access locks	☐	Video systems
☐	Light barriers/motion detectors	☒	Security locks
☒	Key regulations (key issuance etc.)	☐	Identity check carried out by the gatekeeper/reception
☐	Logging visitors	☐	Careful selection of cleaning staff
☐	Careful selection of security staff	☐	Obligation to wear authorisation permits at all times
☒	Magnetic or chip card transponders	☐	Factory security and/or gatekeepers
☒	Electric door openers	☐	Fenced premises
☒	Restriction of those with access authorisation	☐	

Entry Control

Measures suitable to protect the use of the data processing systems by unauthorised persons.

☒	Allocation of user rights	☒	Creation of user profiles

☒	Password allocation	☒	Authentication via biometric procedures
☒	Two-factor authentication	☒	Allocation of user profiles to IT systems
☐	Locking for housing	☒	Use of VPN technology
☐	Blocking external interfaces (USB etc.)	☐	Mobile data carrier encryption
☒	Use of intrusion-detection systems	☒	Laptop/notebook encryption
☒	Use of anti-virus software	☒	Encryption of smartphone contents
☒	Use of a hardware firewall	☐	Use of Mobile Device Management (MDM)
☒	Use of a software firewall	☒	Password guidelines incl. –password length and change
☒	Authentication with user name/password	☒	Automatic locking of monitors
☒	Central data storage	☒	Secure encryption of the hard disks

Access Control

Measures that ensure that those authorised to use a data processing system can only access the data allocated to their particular access authorisation, and that personal data cannot be read, copied, modified or removed without authorisation during the processing, use and following storage.

☒	Creation of an authorisation concept	☒	Management of rights by system administrators
☒	Reduced number of administrators	☒	Password guidelines incl. –password length and change
☒	Logging access to applications, particularly upon entry, change and deletion of data	☒	Secure storage of data carriers
☐	Physical deletion of data carriers prior to re-use	☒	Proper deletion of data carriers (DIN 66399)
☒	Use of document shredders or service providers	☐	Logging of destruction/deletion
☐	Encryption of data carriers	☒	Differentiated access per user as per his/her tasks
☒	Access rights in the file system	☒	Monitoring user logins (when/where the login took place)

Separability

Measures that ensure that data collected for different purposes can be processed separately.

☐	Physically separate storage on specific systems or data carriers	☐	Logical client separation (software side)
☒	Creation of an authorisation concept	☐	In the case of pseudonymised data: Separation of the allocation file and storage on a separated, secured IT system
☐	Equipping the data sets with purpose attributes/data fields	☒	Separation of productive systems and test systems
☐	Determination of database rights	☐	

Pseudonymisation

Measures for processing personal data in such a way that such data can no longer be associated with a specific data subject without the retrieval of additional information, insofar as this additional information is specially stored and is subject to the corresponding technical and organisational measures.

☐	Pseudonymisation of personal data for remote maintenance	☐	Pseudonymisation of data for statistical evaluations

Integrity

Transfer Control

Measures that ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during its transport or storage on data carriers, and that facilitate the monitoring and determination of the points at which the transfer of personal data is planned using devices for data transmission.

☒	Installation of dedicated lines and/or VPN tunnels	☐	Transfer of data in anonymised or pseudonymised form
☐	Email encryption	☐	Creation of an overview of regular access and transfer processes
☐	Documentation of the data recipients and the times of the planned transfer and/or agreed deletion deadlines	☐	In the event of physical transport: secure transport containers/packaging
☐	In the event of physical transport: careful selection of transport staff and vehicles	☒	Encryption of the tunnel connections used upon external access
☒	Secure encryption of the hard disks in the systems of all members	☐	

Input Control

Measures which ensure that it is subsequently possible to monitor and determine if, and by whom, personal data has been entered into, modified or removed from data processing systems.

☒	Logging the input, modification and deletion of data	☒	Creation of an overview displaying with which applications which data can be entered, modified and deleted.
☒	Traceability of the input, modification and deletion of data via individual user names (not user groups)	☐	Storage of forms from which data is taken for automatic processing
☒	Allocation of rights to input, modify and delete data on the basis of an authentication concept	☐	Permanent logging of the remote maintenance sessions via Teamviewer
☒	Access and change history	☐	

Accessibility and Capacity

Accessibility Control

Measures guaranteeing that personal data is protected against destruction or loss.

☒	Uninterrupted power supply (UPS)	☒	Air conditioning in server rooms
☒	Devices to monitor temperature and moisture in server rooms	☒	Protected power outlet strips in server rooms
☒	Fire and smoke alarm systems	☐	Fire extinguishing devices in server rooms
☒	Alarm notification in the case of unauthorised access to server rooms	☒	Creation of a back-up and recovery concept
☒	Data reproduction testing	☐	Creation of an emergency plan (Business Continuity Plan)

☐	Storage of data protection in a secure, outsourced location	☒	Server rooms not beneath sanitary systems
☒	In high-water areas: Server rooms above the waterline	☐	Regular (external) penetration test
☐	Up-to-date IT emergency handbook	☐	Use of a three-step back-up procedure
☐	Data mirroring in separated building/fire sections	☒	Spatially separated storage of the back-up media
☒	Virus protection on all clients and all servers	☒	Redundant hardware firewall present
☐	Emergency power system: Integrated emergency diesel power unit	☒	Redundant computer centre air conditioning available

Recoverability

Measures guaranteeing that installed systems may, in the event of interruption, be restored immediately.

☒	Regulated authorisations for procurement and purchase	☒	Use of a multi-step back-up procedure with comprehensive back-up
☒	Company-wide leave and replacement regulation	☒	Uniformly valid back-up procedure simplified, necessary back-ups if required

Procedure for Regular Monitoring, Assessment and Evaluation

Data Protection Management

Directive(s), guidelines, work instructions and security concepts

☐	Annual auditing by auditors	☒	Continuous monitoring of network components via central auditing solutions incl. alerting
☐	Data protection handbook, work instructions, procedural instructions integrated in the QMS	☐	

Incident Response Plan (Incident Response Management)

Regular checks, documentation and, if necessary, optimisation

☒	Documentation of the data protection carried out	☐	Annual internal data protection audit
☐	Regular data protection checks	☐	Documented standard specifications for configurations in the Intranet
☐	Inspections by the Data Protection Officer	☐	

Data Protection-Friendly Default Setting

Regular checks, documentation and, if necessary, optimisation

☒	Data protection-compliant software solution (privacy by design)	☒	Comprehensive rights and roles concept
☒	Data protection-friendly basic configuration (privacy by default)	☐	

Mandate Inspection

Measures guaranteeing that personal data processed within a mandate are only processed according to the instructions of the principal.

☒	Selection of the contractor subject to due diligence (particularly with regard to data security)	☐	Prior testing and documentation of the contractor’s security measures
☒	Written instructions to the contractor (e.g. via a Job Processing Contract as per Art. 28 GDPR)	☒	Obligation of the contractor's employees to adhere to data secrecy and confidentiality
		☒	Ensuring the destruction of data following the end of the contract
☒	Effective rights of control over the contractor agreed	☐	Continuous monitoring of the contractor and their activities
☐	Contractual penalties in the case of infringements	☐	Formalised contractual relationship and control of the TOMs