DATA PROCESSING ADDENDUM *(SCAN 2X ONLINE SERVICES-CANON (UK) LIMITED DIRECT CUSTOMER VERSION)*

This Data Processing Addendum ("Data Processing Addendum") forms part of and supplements the Contract entered into between Us and You governing Your use of the Online Services known as Scan2x Online.

1. GENERAL

1.1. **Incorporation**: This Data Processing Addendum is in addition to and applies to the contractual relationship between Us and You and the terms set out herein are incorporated into the Contract.

1.2. **Conflict:** In case of a conflict between the terms of this Data Processing Addendum and the Contract, the terms of the Data Processing Addendum shall prevail to the extent of any inconsistency only.

1.3. **Definitions:** In this Data Processing Addendum, expressions defined in the Conditions and used in this Data Processing Addendum have the meaning set out in the Contract, where applicable, or are as set out in this Data Processing Addendum.

1.4. **Rules of Interpretation:** The rules of interpretation set out in the Conditions apply to this Data Processing Addendum.

2. SCOPE

2.1. This Data Processing Addendum shall apply to the processing of Customer Personal Data by Us pursuant to the Contract.

3. PROCESSING REQUIREMENTS

3.1. Unless otherwise set out in the Agreement or in Statements of Work or Purchase Orders submitted under the Contract, details about the Customer Personal Data to be processed by Us and the processing activities to be performed under this Data Processing Addendum are set out in Schedule 1.

3.2. We shall only process Customer Personal Data in accordance with the documented instructions given from time to time by You, including with regard to transfers, unless required to do so otherwise by applicable law. In which event, We shall inform You of the legal requirement before processing Customer Personal Data other than in accordance with Your instructions, unless that same law prohibits Us from doing so on important grounds of public interest.

3.3. Where You are also procuring the Services for one or more of Your Affiliates, You confirm that You are authorized to communicate any instruction or other requirements on behalf of such Affiliates to Us in respect of the Services.

3.4. If You are in breach of Your obligations under the Data Protection Legislation due to Our act or omission, We shall not be liable for such breach where such act or omission arose from Your instructions.

3.5. Upon termination or expiry of the Services, We shall, at Your request, promptly delete or return all Customer Personal Data and delete the copies thereof (unless applicable law requires the storage of such Customer Personal Data) and shall confirm to You in writing that We have done so. This is without prejudice to any provisions in the Contract relating to how long We may retain data after the Contract terminates. This is also without prejudice to Our rights to erase Customer Personal Data under clause 48.4 of the Conditions if You fail to provide such instruction within one month after termination of the Services.

4. SECURITY

4.1. We warrant and undertake in respect of all Customer Personal Data that We shall:

4.1.1. implement appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful processing against accidental loss, destruction, damage, alteration or disclosure, including those measures specified in Schedule 2 and as may be updated from time to time;

4.1.2. without prejudice to any general obligations relating to confidentiality in the Conditions, ensure that Our personnel are subject to binding obligations of confidentiality with respect to Customer Personal Data; and

4.1.3. promptly, and without delay, notify You in writing of any actual, alleged, or potential unauthorised disclosure, loss, destruction, compromise, damage, alteration, or theft of Customer Personal Data.

4.2. You shall promptly and without delay notify Us in writing if You become aware of any breach of security in respect of the Services or Your use of the Services.

5. ASSISTANCE

5.1. Taking into account the nature and scope of the Services provided by Us, We shall, to the extent possible, provide such assistance as You may reasonably require to comply with Your obligations as a data controller, including in relation to data security, data breach notification, data protection impact assessment, prior consultation with data protection authorities, any enquiry, notice or investigation received from a data protection authority, and the fulfilment of data subjects' rights.

5.2. We shall make available to You all information reasonably necessary to demonstrate Our compliance with the obligations set out in this Data Processing Addendum, and allow for and co-operate with any audits, including physical inspections of Our premises, required by You. You shall be limited to conducting one such audit or inspection per year, save where You reasonably believe that We may have breached the provisions of this Data Processing Addendum. Any such audit or inspection shall be conducted on reasonable notice during normal business hours. We may require that the people conducting the audit sign undertakings of confidentiality. Should the inspector appointed by You be in a competitive relationship with Us, We have a right of objection against them. The expenses incurred by Us for any such audit shall be borne by You.

6. SUB-PROCESSING

6.1. You provide Us with a general authorisation to appoint Sub-Processors to process the Customer Personal Data provided that You are: (i) informed of the identity of the Sub-Processor and are given reasonable notice of no less than 30 days in advance of any proposed changes concerning the addition or replacement of other Sub-Processors; (ii) given the opportunity to object to such changes where You consider that such Sub-Processors do not provide sufficient guarantees under Data Protection Legislation in which event We shall use reasonable endeavours to address Your concerns. If You fail to object within the 30 days' notice period, You will have been deemed to accept the appointment and/or replacement of the new sub-processor. You hereby authorise Us to use Sub-Processors: (i) expressly authorized in the Contract; (ii) listed in Schedule 3 of this Data Processing Addendum or (iii) that are Our Affiliates

6.2. We shall impose obligations on Our Sub-Processors that are equivalent to those set out in this Data Processing Addendum by way of written contract (including where Customer Personal Data may be processed outside the United Kingdom / European Economic Area), and We shall remain liable to You for any failure by a Sub-Processor to fulfil its obligations in relation to the Customer Personal Data.

7. DATA TRANSFERS

7.1. Where We appoint Sub-Processors in accordance with paragraph 6 above, We shall put in place terms with Our Sub-Processors to ensure that such Customer Personal Data is only processed in accordance with Your instructions in connection with the Contract with You and shall include adequate safeguards which satisfy the requirements of the Data Protection Legislation (as defined in the Contract) in relation to any processing of Customer Personal Data that may be undertaken by Our Sub-Processors outside of the United Kingdom and/or European Economic Area. Such adequate measures may include:

7.1.1. processing in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or

7.1.2. appropriate safeguards to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Data Protection Legislation, including a transfer mechanism that enables compliance with cross-border data transfer provisions under applicable Data Protection Legislation.

8. LIABILITY

The provisions on the parties' liability contained in the Contract shall be valid also for the purposes of processing under this Data Processing Addendum, unless expressly agreed upon otherwise.

SCHEDULE 1

DESCRIPTION OF THE PERSONAL DATA PROCESSING

The data processing activities carried out by Us pursuant to the Contract and this Data Processing Addendum may be described as follows:

1 Subject Matter

Our provision of the Scan 2x Online Services, related Online Services Support and Implementation Services, to You as described in the Contract.

2 Duration

For the duration of the Contract and the period from the end of the Contract until You revoke Our access to Customer Personal Data or We delete such Customer Personal Data in accordance with the retention period of this Schedule 1.

3 Nature and Purpose

We will process Customer Personal Data for the purpose of providing the Scan 2x Online Services, related Online Services Support and Implementation Services, in accordance with the Contract.

4 Data Categories

Personal Data relating to individuals provided to Us by, or at the direction of, You to receive the Scan 2x Online Services, related Online Services Support and Implementation Services.

As a document capture solution any information you may capture, store, or process could contain any category of personal data including special categories.

Personal data could include for example but is not limited to: name, contact details such as an email address, network information, account information, user ids

Personal data could include special categories of personal data the extent of which is determined and controlled by You. For clarity, these special categories of Personal data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

5 Data Subjects

Data subjects include the individuals about whom Customer Personal Data is provided to Us by, or at the direction of, You to receive the Scan 2x Online Services, related Online Services Support and Implementation Services.

6 Retention Periods

We will retain Customer Personal data for only as long as it is needed for the purpose of providing the contracted service and in accordance with any retention periods required by applicable laws.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL SECURITY MATTERS

1. PROVISION OF SCAN2X ONLINE SERVICES:

1.1. Secure Communication and Vulnerability Management:

All internal communication between the systems is only open to the internal network itself which is protected with a Microsoft Azure firewall. All external communication is encrypted with HTTPS.

1.2. Personal Data Collection and Usage:

While Scan 2x Online Services allows You to extract any information from Your documents and manage that information in the Scan 2x Online Services, We and our Sub-Processors do not specifically have access to that data.

1.3. User Authentication and Password Management:

As part of the Scan 2x Online Services You receive We provision for You an independent, secure Microsoft Azure Active Directory which is managed by Your administrator via the Scan 2x Online Services portal. Your administrator can create new users with passwords or invite users with existing Microsoft accounts (no additional password). Authentication to the Scan 2x Online Services portal and its components is done with OAuth open standard allowing for token-based authentication and authorisation providing single sign-on (SSO).

1.4. Tenant Isolation:

Each Scan2x Online Services tenant is logically separated from other tenants via tenant isolation ensuring no Customer Personal Data is exposed or open to data from other accounts. Customer Personal Data is stored in Scan2x Online Services according to statutory requirements.

1.5. Secure-by-Design Cloud Architecture:

The Scan 2x Online Services components have been built with security in mind and is deployed across a three-tier cloud architecture, with defined network segmentation that is controlled through multiple firewalls. Customer Data is placed on the third (and deepest) level of this architecture, stored in an ISO27001 and PCI DSS compliant DBaaS (Database as a Service) built on Microsoft Azure Cloud Storage. The Scan 2x Online Service in its entirety is regularly security audited by independent security specialists.

1.6. Data Centre:

The applications, databases, documents and related information are all hosted and stored in European data centres.

1.7. Role Concept:

Scan 2x Online Services utilises the 'separation of duties' concept. System administrators can define and assigns roles to users to manage their access to all objects such as folders, categories, cases and documents. This ensures that information is only available to authorised users.

1.8. Additional services:

Scan2x Online Services can exchange information with external services via secure API calls (as defined by system administrator). It is Customer's responsibility to ensure Data Protection Legislation is adhered

to where external services are connected to and Customer Personal Data is shared outside Scan2x Online Services.

2. PROVISION OF ONLINE SERVICES SUPPORT AND IMPLEMENTATION SERVICES

2.1. Physical Access Controls:

- Unauthorized persons are prevented from gaining physical access to the premises, buildings, or rooms where data processing systems that process and/or use Customer Personal Data are located.
- All the buildings or facilities used by Our providers to host IT systems, IT devices, Servers and other critical IT equipment which are used to process or store Customer Personal Data are protected by appropriate physical and environmental controls.

2.2. System Access Control:

Systems processing Customer Personal Data can only be accessed with Authorisation. We protect Our systems and controls using the following measures:

- IT Networks (except for those which are owned or controlled by You) used by Us to process or store any Customer Personal Data have:
  - properly managed, configured and up to date firewalls in place
  - properly managed and configured network monitoring and logging in place
  - properly managed, configured and up to date intrusion detection and/or intrusion prevention systems in place
  - strong access controls in place
  - appropriate levels of redundancy are in place
- Our IT devices, mobile computer devices and Servers used by Us to process or store Customer Personal Data have:
  - anti-virus, anti-malware and anti-spyware software installed and maintained
  - password protection which fulfils Our defined minimum requirements
  - Multi Factor Authentication (MFA) is used where applicable
  - automatic device lock after a period of inactivity
  - appropriate patch management procedures
  - encryption enabled which encrypts any Company Personal Data
- Authorization to critical systems or sensitive information is strictly maintained in accordance with Our security policies.
- All personnel access Our systems with a unique identifier (user ID) and must not be shared
- We have established a password policy that prohibits the sharing of passwords, governs responses to password disclosure

2.3. Data Access Control:

Persons entitled to use data processing systems gain access only to the Customer Personal Data that they have a right to access, and Customer Personal Data must not be read, copied, modified, or removed without authorization in the course of processing, use and storage. Customer Personal Data access is controlled using the following measures:

- As part of the Our security policy, Customer Personal Data requires at least the same protection level as "confidential" information.
- Access to Customer Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require to fulfil their duty.
- We have Data Processing Agreements with Our sub processors involved in the support and implementation services

2.4. Data Transmission Controls:

Customer Personal Data in transfer over Our internal networks and between Us and sub processors or data centres used by Us is appropriately secured.

- All Customer Personal Data which is sent in transit by Us between Your and/or sub processor is sent via secure channels (for example, VPN, Secure FTP or TLS) or encrypted email.
- All encryption used by Our sub processors must satisfy or better the requirements of Our encryption policy

2.5. Data Input Controls:

Measures which make it possible to retrospectively examine and establish whether and by whom Customer Personal Data have been entered, modified, or removed from Our data processing systems:

- We only allow authorized personnel to access Customer Personal Data as required in the course of their duty.
- We have implemented a logging system for input, modification, and deletion, or blocking of Customer Personal Data by Us or Our Sub-Processors within Our Service to the extent technically possible.

2.6. Job Control:

Customer Personal Data is being processed in accordance with the Contract and Your related instructions as follows:

- We use controls and processes to monitor compliance with contracts entered between Us and You, Sub-Processors or Our other service providers respectively.
- All Our employees and contractual Sub-Processors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Our customers and partners.
- Where legally required to do so, we and our service providers, have appointed a Data Protection Officer (DPO) in accordance with the relevant Data Protection Legislation.
- Data Protection Legislation training for all employees is mandatory and is undertaken on a regular basis

2.7. Availability Control:

Customer Personal Data will be protected against accidental or unauthorised destruction or loss

- Our servers are backed up on regular basis which are handled according to Our IT policies
- Where Our applications are hosted on 3rd party server, the cloud hosting provider availability controls and continuity plans apply (i.e. Microsoft Azure, Amazon AWS)
- Appropriate procedures are in place for the vetting of all new applications and service providers used by Us to process or store Customer Personal Data from privacy and security perspective.

2.8. Data Separation Control:

We use appropriate technical controls to achieve Customer Personal Data logical separation.

- Full separation (where applicable) of the service providers production and development / test / training environments is in place
- Appropriate separation controls are in place which provide for the separation of different customers data on Our IT hardware and software
- Customer Personal Data is processed by Us as separately as possible from the Our other customer's data.

2.9. Data Integrity Control:

Customer Personal Data will remain intact, complete and current during processing activities:

- We have implemented a multi-layered defence strategy as a protection against unauthorized modifications, in particular by implementing the measures described above.

SCHEDULE 3

APPROVED SUB-PROCESSORS

Sub-Processor Name	Purpose	Location	Address
Canon Europa N.V.	Online Software, Hosted System Reseller	The Netherlands	Bovenkerkerweg 59,1185 XB Amstelveen, The Netherlands
Avantech Software	Online Software, Hosted System Provider and Online Services Support	Malta	Avantech Buidling, St., Julians Road, San Gwanns SGN 2804, Malta
Teleperformance	Online Services Support	Greece	330 Thisseos Avenue, 17675 Athens, Greece