PERSONAL DATA PROCESSING APPENDIX

This Basware personal data processing appendix and its annexes (**"DPA"**) is an appendix to, and legally binding only in connection with, the sales agreement between **Basware** and **Customer** with regard to Basware Cloud Services and related Professional Services (**"Agreement"**) that references this DPA. Capitalized terms used but not defined in this DPA shall have the meaning specified in the Agreement. Any non-capitalized term related to processing of Personal Data (as defined below) used but not defined in this DPA shall have the meaning specified under the Data Protection Laws (as defined below).

1. PREAMBLE and DEFINITIONS

Pursuant to the Agreement, Basware provides Cloud Services and related Professional Services to Customer, as specified in the Agreement. To provide these Services, Customer might require Basware to process Personal Data, on Customer's behalf.

Data Protection Laws mean the Regulation and any other data protection laws to the extent they apply to the related party's operations.
Personal Data means any information relating to an identified or identifiable natural person.
Regulation means the European Regulation (EU) 2016/679 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.
Services means Cloud Services and related Professional Services specified in the Agreement.

2. PERSONAL DATA

To the extent Customer requires Basware to process any Personal Data on Customer's behalf in connection with and for the purpose of providing the Services, both parties shall comply with the provisions of this DPA. In the context of the Agreement, Personal Data mainly includes, as determined and controlled by Customer in its sole discretion, without being exhaustive, business contact data such as name, title, position, business (email/physical) address and telephone number of Customer's and/or Customer's trading partners' individual representatives in the order and/or invoice data that are processed through the Services. Personal Data may further also include special categories of Personal Data, such as data revealing race, political opinions or religion or health related data.

3. CUSTOMER OBLIGATIONS

3.1. **Controller.** Customer shall be the sole controller for the Personal Data pursuant to the Regulation and shall be responsible for the lawful collection, processing and use, and for the accuracy of the Personal Data, as well as for preserving the rights of the individuals concerned. If and to the extent legally required, Customer shall inform the individuals concerned regarding the processing of their Personal Data by Basware and shall obtain their consent if necessary.

Customer acknowledges that due to the nature of the Services, Basware cannot control and has no obligation to verify the Personal Data Customer transfers to Basware for processing on behalf of Customer when Customer uses the Services. Customer ensures that Customer is entitled to transfer the Personal Data to Basware so that Basware may lawfully process the Personal Data on behalf of Customer.

3.2. **Instructions.** Customer confirms that Customer's instructions (see also clause 4.1) are exhaustively set out in the Agreement. In case Customer subsequently wants to modify its instructions, it shall primarily use the functions offered by the Services. If such functions would however not be sufficient for implementing such new instructions, Customer shall contact Basware in writing. If such new instructions exceed the scope of the Services provided under the Agreement, Customer shall pay an additional reasonable remuneration for such additional Basware activities, based on the actually delivered work. Instructions must be reasonable, compliant with Data Protection Laws and consistent with the Agreement.

4. BASWARE OBLIGATIONS

4.1. **Processor.** Basware, being the processor pursuant to the Regulation, shall, and ensures that its related employees shall, process the Personal Data exclusively on behalf of Customer, as is necessary for Basware to perform its obligations under the Agreement and in accordance with Customer's instructions (see clause 3.2), unless as far as otherwise required by applicable law. Consequently, Basware shall not use the Personal Data for any other purpose and shall not transfer the Personal Data to unauthorized third parties, nor use the Personal Data for its own purposes.

4.2. **Notification.** Basware shall notify Customer without undue delay if it believes that any new instruction issued by Customer (see clause 3.2) violates the Regulation. Basware may suspend the implementation of such new instruction until Customer has modified the instruction or confirmed the instruction is not violating the Regulation. Basware shall not be obliged to verify whether any instruction given by Customer is consistent with applicable laws, as Customer is responsible for such compliance verification of its instructions.

4.3. **Assistance.** To respond to requests from individuals exercising their rights as foreseen in Data Protection Laws, such as the right of access and the right to rectification or erasure, Customer shall first use the corresponding functions of

the Services. Where this is not possible through the Services, Basware shall provide reasonable assistance to Customer, without undue delay, taking into account the nature of the processing. Basware shall further provide reasonable assistance to Customer in ensuring compliance with Customer's obligations to perform security and data protection assessments, security incident notifications (see clause 4.8) and prior consultations of the competent supervisory authority, as set out in the Data Protection Laws, taking into account the nature of the processing and the information available to Basware. Customer shall pay an additional reasonable remuneration to Basware for handling such assistance requests.

In case any individual or supervisory authority makes a request for assistance directly to Basware concerning Personal Data, such as a request for access, rectification or erasure, delivering any information or executing any other action, Basware shall inform Customer on such request as soon as reasonably possible and as far as allowed by applicable law.

4.4. **Location of Personal Data processing.** To provide the Services, Customer accepts that Basware may have Personal Data processed and accessible by its Subprocessors (as defined in clause 6.1) outside Customer's country of domicile. In case the processing is subject to the Regulation and Personal Data is transferred from the European Economic Area (**"EEA"**) to a Subprocessor for processing in any country outside the EEA that is not recognized by the European Commission as providing an adequate level of protection for personal data, Basware provides for appropriate safeguards by standard contractual clauses, adopted or approved by the European Commission and applicable to the processing by the non-EEA Subprocessor as specified in the Data Transfer annex 1 to this DPA, or by any other appropriate safeguard as foreseen under the Regulation.

4.5. **Data protection officer.** To the extent required by mandatory Data Protection Laws, Basware appoints a data protection officer and shall communicate the relevant contact details to Customer upon request.

4.6. **Employees.** Basware familiarizes its employees, authorized to process Personal Data, with relevant statutory data protection regulations, and ensures that these employees have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.7. **Technical and organizational security measures.** Basware implements and maintains the appropriate technical and organizational security measures to protect Personal Data within its area of responsibility as detailed in annex 2 to this DPA. Basware may modify its security measures from time to time but will not decrease the overall security during the term of the DPA.

4.8. **Security incident notification.** In the event of any security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed by Basware, Basware shall, without undue delay after having become aware of it, notify Customer in accordance with the Data Protection Laws. Such notification shall allow Customer to perform any further notification as legally required.
The security incident notification shall at least contain the following information:

(a) description of the nature of the security incident, including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of Personal Data records concerned;
(b) name and contact details of Basware's contact point where more information can be obtained;
(c) description of the likely consequences of the security incident; and
(d) description of the measures taken by Basware to address the security incident, including, where appropriate, measures to mitigate its possible adverse effects.

In so far as it is however not possible to provide the information listed above at the same time, the information may be provided in phases without undue further delay.

Basware shall document any security incident, including the related facts, its effects and the remedial action taken. To the extent the security incident results from Basware's breach of the Agreement, Basware will use commercially reasonable efforts to remediate the cause of such security incident.

4.9. **Record of processing activities.** Basware maintains a record of all categories of Personal Data processing that are subject to the Regulation, carried out on behalf of Customer. This record contains the information as required by the Regulation.

5. AUDIT

5.1. **Documentation.** To the extent required by Data Protection Laws, Basware has documented the activities taken to ensure compliance with its obligations under this DPA. Upon request, Basware shall present to Customer a copy of the relevant part of such documentation relating to this DPA and the processing activities carried out under this DPA.

5.2. **Audit.** To the extent further required by Data Protection Laws, Customer may audit Basware's compliance with its obligations under this DPA. Customer shall announce in writing any audit on the premises of Basware two weeks in advance. In consideration of an audit on Basware's Cloud Service related systems, Basware will create a test platform where the Customer can perform the audit. Audits must be carried out during normal business hours and without causing significant disturbances to the business operations of Basware.

5.3. **Costs.** Upon Customer's request, Basware will provide a copy of the documentation referred to in clause 5.1 and any existing documentation relevant to the audit, free of charge. For any additional documentation, support or service requested by Customer, Basware reserves the right to invoice the Customer all reasonable costs directly arising from such Customer requests. This shall also include adequate compensation for the working hours of Basware staff while they are supporting Customer's audit, unless as far as the audit reveals that Basware does not comply with its obligations under this DPA.

5.4. **Protection of Basware's interests.** Where an audit may lead to the disclosure of business or trade secrets of Basware or threaten intellectual property rights of Basware or in any other case at Customer's discretion, Customer shall employ an independent expert to carry out the audit, and the expert shall agree to be bound to secrecy to Basware's benefit.

6. SUBPROCESSORS

6.1. **General authorization.** Customer gives its general authorization to allow Basware to involve Basware's affiliated companies and other Subcontractors as subprocessors to process Personal Data in connection with the provision of the Services (**"Subprocessors"**), to the extent such appointment does not lead to non-compliance with any applicable law or Basware's obligations under this DPA. Basware ensures that the involved Subprocessors are properly qualified, will be under a data processing agreement with Basware and comply with data processing obligations similar to the ones which apply to Basware under this DPA. Basware regularly monitors the performance of its Subprocessors and is liable for their work towards Customer.

6.2. **Change of Subprocessor.** Basware is free to choose and change Subprocessors. Upon request, Basware shall inform Customer of the main Subprocessors currently involved. In case there is a later change of any main Subprocessor (addition or replacement), Basware shall notify Customer of such change. Should the processing be subject to the Regulation and should Customer reasonably demonstrate that such new Subprocessor has breached, or is likely to breach, the Regulation and therefore not be able to support the involvement of that new Subprocessor, Basware will undertake reasonable efforts to remedy this situation. Should this not be remedied and Basware continues to involve the related new Subprocessor for the Services, Customer shall be entitled to terminate the related part(s) of the Agreement for which the related new Subprocessor is involved, subject to three (3) months' prior notice, without any compensation or exit penalty being due by Basware. To avoid any misunderstanding, should Customer not exercise this right of termination, it shall be deemed to support the involvement of the related Subprocessor and Basware confirms to continue to be liable for this Subprocessor's work towards Customer, in accordance with clause 6.1.

7. TERM

7.1. **Term.** This DPA shall apply until the effective date of the termination of the Agreement. To the extent Personal Data is processed by Basware after the effective date of termination of the Agreement, for whatsoever legitimate purpose, the terms of this DPA shall continue to apply to such processing for as long as such processing is carried out.

7.2. **Personal Data at the end of the DPA.** During a limited period of time from the date when the provision of the Cloud Services ends, Basware shall make Customer Data (containing Personal Data) available to Customer as further specified in the Agreement. Within a reasonable time after expiry of the above-mentioned limited period of time, Basware shall permanently delete Customer's Personal Data from its storage media, except to the extent that Basware is under a statutory obligation to continue storing such Personal Data. On Customer's request, Basware shall confirm the deletion in writing.

8. MISCELLANEOUS

8.1. **Customer Affiliates.** Both parties acknowledge and agree that Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Affiliates that use the Services, if and to the extent Basware processes Personal Data for which such Customer Affiliates qualify as data controllers as meant in clause 3.1. For the purposes of this DPA only, the term "Customer" includes Customer and its above meant Affiliates. To the extent this DPA is concluded on behalf of Customer Affiliates as meant above, the liability cap specified in the Agreement shall, with regard to Basware's liability under this DPA, be applied in aggregate, in a combined manner, to all claims together of Customer and concerned Customer Affiliates, related to the same event giving rise to liability, and shall not be understood to apply individually or severally to Customer and/or any of its concerned Affiliates.

8.2. **Indemnity.** Subject to the liability cap mentioned in the Agreement, Basware shall indemnify Customer and Customer shall indemnify Basware for (i) administrative fines paid by the indemnified party and imposed on it by the competent supervisory authority, and (ii) damages paid by the indemnified party to natural persons based on a settlement (agreed by the indemnifying party) or final judgement, if the claim against the indemnified party results from breach of this DPA or any Data Protection Law by the indemnifying party, and only to the extent such breach is attributable to the indemnifying party. The indemnifying party shall provide, at its own cost, all reasonable support to the indemnified party in defending the claim. This clause 8.2 provides the indemnified party's exclusive remedy for all claims against it by any competent supervisory authority and natural persons.

8.3. **Compliance with laws.** Either party shall comply with the provisions of the Data Protection Laws as far as they apply to its operations. In the event any such statutory provision requires this DPA to be amended, upon request of either party, the necessary amendments shall be discussed in good faith, documented in writing and duly signed by both parties.

8.4. **Order of precedence.** This DPA is subject to the Agreement, to which it is added as Appendix. Any provision related to the processing of Personal Data by Basware that is mentioned in the Agreement (not including this DPA) will be replaced with the present DPA as of its signature by both parties. In case of conflict between this DPA (not including annex 1) and annex 1, the provisions of annex 1 shall prevail.

9. ANNEXES

The below-listed annexes are incorporated into this DPA by this reference:

- Annex 1: Data Transfer Annex
  A – Cover Note
  B – Standard Contractual Clauses (processors)
- Annex 2: Basware Services Technical and Organizational Security Measures

ANNEX 1: DATA TRANSFER ANNEX

A – Cover Note

1. This Cover Note (A) and the Standard Contractual Clauses (B) together constitute the "**Data Transfer Annex**" to the Personal Data Processing Appendix between Basware and Customer, as part of the Agreement.

2. This Data Transfer Annex is only **applicable** as far as the processing of Personal Data as meant under the Personal Data Processing Appendix is subject to the Regulation and Personal Data is transferred for processing to the Subprocessor identified in the Standard Contractual Clauses.

3. Under the Standard Contractual Clauses, Customer (being controller under the Personal Data Processing Appendix and the Regulation) qualifies as **data exporter** and each identified Subprocessor qualifies as **data importer**.

4. In accordance with the Personal Data Processing Appendix, Basware provides for appropriate safeguards by the **Standard Contractual Clauses**, applicable to the processing by the specified data importer and subject to the following additional clarifications:
   a) For the purposes of clause 5(a) of the Standard Contractual Clauses, data exporter's instructions are described in the Personal Data Processing Appendix.
   b) For the purposes of clauses 5(f) and 12(2), the audit shall be carried out in accordance with the Personal Data Processing Appendix.
   c) For the purposes of clauses 5(h) and 11 of the Standard Contractual Clauses, data exporter's general authorization for subprocessing is described in the Personal Data Processing Appendix. The copy of any subprocessor agreement that must be sent to the data exporter pursuant to clause 5(j) of the Standard Contractual Clauses, may have any commercially sensitive information removed by Basware beforehand, and will only be sent to data exporter upon the latter's request.

5. Parties acknowledge and agree that Customer enters into this Data Transfer Annex on behalf of itself and, to the extent required under the Regulation, in the name and on behalf of its **Affiliates** that use the Basware services under the Agreement, if and to the extent data importer processes Personal Data for which such Customer Affiliates qualify as controllers and data exporters as meant in clauses 2 and 3 above. For the purposes of this Data Transfer Annex only, the terms "Customer" and "data exporter" include Customer and its above meant Affiliates.

B – Standard Contractual Clauses (processors)

By executing the Agreement, Customer grants a **power of attorney** entitling Basware Corporation [Linnoitustie 2, 02601 Espoo, Finland] to execute the EU Standard Contractual Clauses (processors) (cf. *European Commission Decision of 5 February 2010, 2010/87, including its applicable amendments and replacements*), on Customer's behalf, with any Subprocessor to the extent the latter qualifies as data importer under the Agreement and the present Data Transfer Annex applies.

Basware makes a copy of the signed EU Standard Contractual Clauses available to the Customer.

ANNEX 2: BASWARE SERVICES TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Basware may modify its security controls from time to time but will not decrease the overall security during the term of the Agreement.

SECURITY CONTROLS

1. **Risk Management.** Basware assesses risks related to the Services as part of Basware's Corporate Risk management process and manages these according to related management practices. Risk management process is included in Basware's Information Security Management system.

2. **Information Security Management.** Basware has an Information Security Management System (ISMS) that is aligned to industry best practices such as ISO 27001 and includes Security Policies, organization, processes and controls meeting compliance and security requirements identified by Basware.

3. **Personnel Security.** Basware implements processes for hiring, maintaining and terminating contracts with individual employees. Basware employs role specific security activities such as background screening, continual security awareness, physical and logical access management, meeting identified risks, security requirements and applicable legal requirements and restrictions to those roles.

4. **Asset Management.** Basware processes Customer Data in accordance with the Agreement, including relevant Service Documentation. Basware may manage IT resources included in Service delivery according to Basware internal classification and processes (e.g. production and test environments).

   Where data or assets is set to be deleted and disposed, Basware follows a set process to ensure the equipment and storage media is properly sanitized before physical disposal.

5. **Access Management.** Basware's Cloud Services are protected using both network and logical level security solutions. Basware utilizes industry standard cloud security solutions as well as third party security products and services within the Cloud Service environment. Administrative access to the Service environment requires separate authorization and use of dedicated administrative tooling.

   Responsibility for cloud access is divided between Customer and Basware. Basware controls its access and authorization to Cloud Services. Basware manages accounts under its responsibility using the principle of least privilege based on access requirements of the defined job roles. Customer is provided with mechanisms to maintain its access, authorization and authentication.

   Where Service delivery requires access to Customer systems and assets and Customer grants access to these, Basware personnel abides to the related instructions of Customer for the access management and conduct. It is at Customer responsibility to ensure such instructions are provided to the related Basware personnel in writing.

6. **Encryption.** Network traffic over public Internet is encrypted. Basware supports industry best practice for ciphers and key lengths. Customer Data is stored encrypted.

7. **Physical Security.** Basware provides the Services in co-operation with its hosting service provider. The hosting service provider defines and maintains the physical and environmental controls for production environments. The provider has assurance reports and security certifications covering these controls and additionally these controls are under regular Basware scrutiny.

8. **Operations Security.** Basware follows industry best practices like automation and vendor recommendations where applicable to configure cloud environments securely used by the Services. Basware uses automated and manual activities to keep software in use updated and address reported vulnerabilities.

9. **Vulnerability Management.** Basware uses several sources such as vulnerability scanning, security testing and threat intelligence to identify potential vulnerabilities in the Services. Reported vulnerabilities are assessed and addressed using defined processes and activities. Basware provides a responsible disclosure channel for security researchers to report any found issues in the Services.

10. **Security Testing and Audits.** Basware co-operates with a third-party security services company to regularly carry out penetration testing. Findings and other results of the testing are managed using Basware vulnerability management processes and activities. Security testing results are Basware company confidential and internal to Basware.

11. **Security Event Management.** Basware monitors the Cloud Services environments using several logging and monitoring tools to identify events and incidents affecting the Cloud Services. Security event related incidents are managed by operational processes supported by Basware's Security Team.

12. **Service Resilience.** The Services are designed to comply with the agreed Service levels. Solutions therefore include the use of fault tolerant and scalable services provided by Basware's hosting service provider or application architecture solutions such as clustering and dedicated services enabling load balancing during high load situations. Protective measures for denial of Service attacks are employed.

Basware Cloud Service deployments are in Europe (EU), United States (US) and Australian (AU) regions utilizing multiple data center units available within the given region ensuring service availability in the unlikely event of a data center not being available.

13. **Business Continuity and Backups.** Customer Data is backed up and restoration of the back-ups are tested regularly to ensure Basware can meet its recovery-point objective (RPO) and recovery-time-objective (RTO) commitments as per Service Documentation.

14. **Endpoint Security.** The Services receive and deliver documents to and from Customer environments. Customer documents are scanned using anti-malware solutions when stored and processed within Basware environments. Documents detected to contain malware may be quarantined or deleted depending on the case. Where applicable, Basware provides reports for such rejected documents to Customer.

Relevant Service components (e.g. servers) are also scanned for malware and monitored to detect malicious programs and files.

Basware office environments are equipped with malware protection for workstations, internal servers, email attachments and other collaboration tools.

15. **System Development.** Basware develops new features and fixes to reported issues following the Product Management and R&D development processes. Security and compliance requirements are managed as part of product functional and non-functional requirement management. Separate environments are used for Service development, testing and quality assurance and delivering production Services.

16. **Assurance and Supplier Management.** The Service environment has a defined control set for development, testing, deployment and maintenance processes. Basis for these controls are the AICPA Trust Service Criteria and ISO 27001 standard. The control environment is externally audited by a well-known certified public accountant (CPA) entity at regular intervals. The results of these audits are available to Basware customers in industry standard report formats.

External third parties provide their own assurance reports on defined control environments, which Basware scrutinizes to ensure the adoption and effectiveness of needed controls.