PERSONAL DATA PROCESSING CLAUSES

DATA TRANSFER ANNEX
FOR
SUBPROCESSORS:
BASWARE INDIA PRIVATE LIMITED, BASWARE INC., BASWARE PTY LTD. AND BASWARE HOLDINGS LIMITED

A - COVER NOTE

1. This Cover Note (A) and the Standard Contractual Clauses (B) that follow this Cover Note together constitute a "**Data Transfer Annex**" to the Personal Data Processing Clauses (i.e. personal data processing appendix or data privacy clauses in the general terms) between Basware [Basware Corporation, Linnoitustie 2, 02601 Espoo, Finland, or any of its affiliates that signed the Sales Agreement with Customer] and Customer, as part of the Agreement for the Services for which Basware involves any of its Subprocessors identified in the following Standard Contractual Clauses.

2. This Data Transfer Annex is **only applicable** as far as the processing of Personal Data as meant under the Personal Data Processing Clauses and the Agreement, is subject to any EU data protection law and Personal Data is transferred for processing to any of the Subprocessors identified in the following Standard Contractual Clauses.

3. Under the Standard Contractual Clauses, Basware's Customer (being controller under the Personal Data Processing Clauses and the EU General Data Protection Regulation (GDPR)) qualifies as **data exporter** and each identified Subprocessor qualifies as **data importer**.

4. Parties acknowledge and accept that Basware is entitled to **publish** a downloadable copy of the present signed Data Transfer Annex (part A and/or part B) on any of its company websites and to deliver such copies to the Customer on request.

PERSONAL DATA PROCESSING CLAUSES

Agreed and signed:

DATA EXPORTER

Customer
Customer's company details on the Sales Agreement with Basware shall apply.

Basware Corporation signs the present Data Transfer Annex on behalf of the Customer for which Personal Data is transferred for processing to any of the following Subprocessors: Basware India Private Limited, Basware Inc., Basware Pty Ltd. and/or Basware Holdings Limited, under the Agreement between Customer and Basware.

Basware Corporation

DocuSigned by:
Klaus Andersen
BA38841703C54A0...

Klaus Andersen
CEO

Address:
Linnoitustie 2,
02601 Espoo,
Finland

DATA IMPORTER 1

Basware India Private Limited

DocuSigned by:
Martti Nurminen
0CD550FB4D71469...

Martti Nurminen
Director

Address:
Rajiv Gandhi IT Park,
DLF Building,
Tower A, ground floor,
160 101 Chandigarh,
India
Tel.: +91 172 3012 020

DATA IMPORTER 2

Basware Inc.

DocuSigned by:
Martti Nurminen
0CD550FB4D71469...

Martti Nurminen
Secretary & Treasurer

Address:
1245 Rosemont Drive,
Suite 200,
Fort Mill,
SC 29707,
USA
Tel: +1 203 487-7900

DATA IMPORTER 3

Basware Pty Ltd.

DocuSigned by:
34D56AD40D7743C...

Michael Pyliotis
Director

Address:
Level 15, 67 Albert Avenue,
Chatswood,
NSW 2067,
Australia
Tel: +61 2 8622 5850

DATA IMPORTER 4

Basware Holdings Limited

DocuSigned by:
Martti Nurminen
0CD550FB4D71469...

Martti Nurminen
Director

Address:
12, New Fetter Lane,
EC4A 1JP London,
UK
Tel: +44 845 6711953

PERSONAL DATA PROCESSING CLAUSES

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE
Directorate C: Fundamental rights and Union citizenship - Unit C.3: Data protection

B - Standard Contractual Clauses (processors)

Execution of the Cover Note (A) of the Data Transfer Annex, to which these Standard Contractual Clauses (B) are attached, on behalf of the **Customer** (data exporter) and **Basware India Private Limited, Basware Inc., Basware Pty Ltd.** and **Basware Holdings Limited** (each in its capacity of data importer) includes execution of these Standard Contractual Clauses (including Appendix 1 and Appendix 2).

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, **Customer** (data exporter) and **Basware India Private Limited, Basware Inc., Basware Pty Ltd.** and **Basware Holdings Limited** (each in its capacity of data importer, whose company details and signature appear above in the Cover Note), each a "party," together "the parties".

HAVE AGREED on the following Contractual Clauses (the "Clauses" or "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result

of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

DS DS DS

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law.

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses.[2] Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

***

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter
Customer is the data exporter. Customer is the user of Basware's services as specified in the Sales Agreement.

Data importer
Basware India Private Limited, Basware Inc., Basware Pty Ltd. and Basware Holdings Limited are each a data importer and a subsidiary of Basware Corporation.
Data importers provide mainly infrastructure maintenance and support, and customer care to Basware's customers worldwide in connection with the provision of Basware's services.

Data subjects
The personal data transferred concern the following categories of data subjects:
individual representatives of data exporter and/or data exporter's trading partners.

Categories of data
The personal data transferred concern the following categories of data:
mainly business contact data, such as, without being exhaustive, name, title, position, business (email/physical) address and telephone number and language.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
data exporter may submit special categories of data to the Basware services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is, for the sake of clarity, personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life or sexual orientation.

Processing operations
The personal data transferred will be subject to the following basic processing activities:
The personal data might be processed by the data importer when providing infrastructure maintenance and support, and customer care to data exporter in connection with the provision of Basware's services.

***

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data Importer (hereinafter referred to as "Basware") may modify its security controls from time to time but will not decrease the overall security during the term of the present Standard Contractual Clauses.

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.

DS DS DS

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.

***