PERSONAL DATA PROCESSING APPENDIX
to implement GDPR legislative obligations

This personal data processing appendix and its annexes (**"DPA"**) is an appendix to, and legally binding only in connection with, each sales agreement currently in place between **Basware** and **Customer** with regard to Basware Services (**"Sales Agreement"**). For this DPA, "**Services**" mean Basware Cloud Services (i.e. made available to Customer via a network) and Basware remotely accessing Customer's data in the on-premise licensed software under its support and maintenance services. The Sales Agreement, together with all its appendices, is jointly referred to as the "**Agreement**".
This DPA is supplemental to the Agreement but replaces any provision in the Agreement relating to the processing of Personal Data (as defined below) by Basware.
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 used but not defined in this DPA shall have the meaning specified under the applicable data protection law.

1. PREAMBLE

Pursuant to the Agreement, Basware provides Services to Customer, as identified in the Sales Agreement. Customer might require Basware to process Personal Data, on Customer's behalf, for the purpose of providing the Services.

2. PERSONAL DATA

To the extent Customer requires Basware to process any information relating to an identified or identifiable natural person on Customer's behalf, in connection with and for the purpose of providing the Services (**"Personal Data"**), both parties shall comply with the provisions of this DPA. 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, telephone number and language 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, as determined and controlled by Customer in its sole discretion, special categories of data, 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.

3. CUSTOMER OBLIGATIONS

3.1. **Data controller.** Customer shall be the sole data controller for the Personal Data pursuant to the EU 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 (the **"Regulation"**) and/or any applicable national data protection law 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 (**"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 the scope of such new Instructions is beyond the Services, Customer shall pay an additional adequate remuneration for such additional Basware activities. Instructions must be commercially reasonable, compliant with applicable data protection laws and consistent with the Agreement.

4. BASWARE OBLIGATIONS

4.1. **Observe Instructions.** Basware, being the data 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, 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 if it believes that any new Instruction issued by Customer (see clause 3.2) violates any applicable data protection law. Basware may suspend the implementation of such new Instruction until it is modified or confirmed by Customer. 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 applicable data protection law, 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 Customer with commercially reasonable assistance, without undue delay, taking into account the nature of the processing. Basware shall further provide Customer with commercially reasonable assistance 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 applicable data protection law, taking into account the nature of the processing and the information available to Basware. Customer shall pay 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 any EU data protection law 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. Moreover, Basware and its Affiliates are party to an intra-group data transfer agreement, containing the EU Article 29 Working Party ad hoc model clauses "EU data processor to non-EU sub-processor", of which Customer can obtain a copy (excluding commercially sensitive information). Customer is responsible for obtaining consents of the related individuals to the extent necessary for the transfer.

4.5. **Data protection officer.** To the extent required by mandatory data protection law, 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 when processed by Basware (**"Security Incident"**), Basware shall, without undue delay after having become aware of it, notify Customer per applicable data protection law. 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. **Records of processing activities.** At the latest as of when the Regulation and the applicable EU member state's data protection law further specifying and implementing the Regulation become enforceable, Basware shall maintain a record of all categories of Personal Data processing that are subject to any EU member state's data protection law, carried out on behalf of Customer. This record contains the information as required by the Regulation and the applicable EU member state's data protection law.

5. AUDIT

5.1. **Documentation.** At the latest as of when the Regulation and the applicable EU member state's data protection law further specifying and implementing the Regulation become enforceable, Basware will have documented the activities taken to ensure compliance with its obligations under the Regulation, the applicable EU member state's data

protection law and this DPA, at Basware's cost. 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, Customer may audit Basware's compliance referred to in clause 5.1. Customer shall announce in writing any audit on the premises of Basware two weeks in advance. In consideration of an audit on Basware's 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.** Basware will provide a copy of the documentation referred to in clause 5.1 and any existing documentation relevant to the audit referred to in clause 5.2, requested by Customer, free of charge. For any additional documentation, support or service requested by Customer, Basware reserves the right to invoice the effort and arising reasonable cost to Customer. 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, 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 Subprocessors currently involved. In case there is a later change of Subprocessor (addition or replacement), Basware shall notify Customer of such change. Should the processing be subject to any EU data protection law and should Customer demonstrate in writing that such new Subprocessor has breached any applicable data protection law and therefore not be able to support the involvement of that new Subprocessor, Basware will undertake commercially 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. The obligation to delete Personal Data shall not apply to Personal Data contained in regular back-up copies of comprehensive datasets from which the individual deletion of Customer's Personal Data would not be possible without significant efforts or costs.

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 applicable 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.

8.2. **Liability.** To the extent this DPA is concluded on behalf of Customer Affiliates as meant in clause 8.1, 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.

8.3. **Indemnity.** Subject to the liability cap mentioned in the Agreement, Basware shall indemnify Customer (subject to the specification in clause 8.2), 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 applicable 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 8.3 provides the indemnified party's exclusive remedy for all claims against it by any competent supervisory authority and natural persons.

8.4. **Compliance with laws.** Either party shall comply with the provisions of the data protection laws that specifically apply to its operations. More particularly, either party shall comply with the requirements of the Regulation and the applicable EU member state's data protection law implementing the Regulation, as of when they become enforceable, as far as they specifically 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.

8.5. **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
- Annex 2: Basware Cloud Services Technical and Organizational Security Measures

PERSONAL DATA PROCESSING APPENDIX
to implement GDPR legislative obligations

On behalf of **Customer** and, to the extent required under applicable data protection laws as specified in clause 8.1, in the name and on behalf of its **Affiliates** that use the Services:	On behalf of **Basware**:
_____ Name	Mr Vesa Tykkyläinen Name
_____ Title / function	Director Title / function
_____ Place	Espoo, Finland Place
_____ Signature	DocuSigned by: Vesa Tykkylainen C4D0A9B8FC79461... Signature
_____ Date of signature	21-Mar-18 Date of signature

ANNEX 1: DATA TRANSFER ANNEX

A - COVER NOTE

1. This Cover Note (A) and the Standard Contractual Clauses (B) that follow this Cover Note 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 any EU data protection law and Personal Data is transferred for processing to the Subprocessor identified in the following Standard Contractual Clauses.
3. Under the Standard Contractual Clauses, Customer (being data controller under the Personal Data Processing Appendix and the Regulation) qualifies as „**data exporter**“ and the identified Subprocessor qualifies as „**data importer**“.
4. Further to and in accordance with clause 4.4 of the Personal Data Processing Appendix, Basware provides for appropriate safeguards by the following 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 clause 3.2 of 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 clause 5 of 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 clause 6 of 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. It is expressly agreed that the data exporter shall exclusively have recourse against Basware for any claims the data exporter might have against the data importer under the present Data Transfer Annex or otherwise under the Personal Data Processing Appendix.
6. Parties acknowledge and agree that Customer enters into this Data Transfer Annex on behalf of itself and, to the extent required under applicable EU data protection laws, in the name and on behalf of its Affiliates that use the Services, if and to the extent data importer processes Personal Data for which such Customer Affiliates qualify as data 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.

Agreed and signed:

On behalf of **Customer** and, to the extent required under applicable data protection laws as specified in clause 6 above, in the name and on behalf of its **Affiliates** that use the Services **(data exporter)**:	On behalf of **Basware India Private Limited (data importer)**:	On behalf of **Basware**:
Customer's signature of the main body of this DPA above and its company details on the Sales Agreement apply.	Name: Mr Niclas Rosenlew	Name: Mr Vesa Tykkyläinen
	Position: Director	Position: Director
	Address: Rajiv Gandhi IT Park, DLF Building Tower F, Third Floor 160 101 Chandigarh India Tel.: +91 172 3012 020 Fax: +91 172 3919 699	Address: (cf. Basware's address on the Sales Agreement)
	DocuSigned by: N. R. Sen 492EA66A566045E... Signature	DocuSigned by: Vesa Tykkylainen C4D0A9B8FC79461... Signature
	21-Mar-18 Date of Signature	21-Mar-18 Date of Signature

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

B - Commission Decision C(2010)593 - Standard Contractual Clauses (processors)

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.

Name and address and contact details of the data exporting organisation: **Customer** identified in the related Sales Agreement

Other information needed to identify the organisation: /

(the data **exporter**)

And

Name of the data importing organisation: **Basware India Private Limited**

Address: Rajiv Gandhi IT Park, DLF Building, Tower F, Third Floor, 160 101 Chandigarh, India.

Tel.: +91 172 3012 020; Fax: +91 172 3919 699.

Other information needed to identify the organisation: /

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the 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

For the purposes of the Clauses:

(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[1];

(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 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.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 to this contract;

(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[2]

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;

(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;

[2] 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.

(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;

(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[3]. 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.

[3] 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.

PERSONAL DATA PROCESSING APPENDIX
to implement GDPR legislative obligations

On behalf of "the data exporter":

Customer's signature of the main body of this DPA above and its company details on the Sales Agreement apply.

On behalf of Basware India Private Limited, "the data importer":
Name: Mr Niclas Rosenlew
Position: Director
Address: Linnoitustie 2, 02601 Espoo, Finland
Other information necessary in order for the contract to be binding (if any): /

DocuSigned by:
Signature..... 492EA66A566045E.....

21-Mar-18
Date of signature.....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
the legal entity that has executed the present Standard Contractual Clauses as data exporter and has purchased Basware Services on the basis of the Sales Agreement.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
a service provider performing automation services for procurement and account payable and receivable processes, and mainly infrastructure support, customer care and, where applicable, scanning validation services, to worldwide customers of its affiliated companies (within Basware Group).

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
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 (please specify):
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 (please specify):
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 (please specify):
The personal data might be processed by the data importer when providing infrastructure support, customer care and, where applicable, scanning validation Services for the benefit of the data exporter.

DATA EXPORTER

Customer's signature of the main body of this DPA above applies.

DATA IMPORTER Basware India Private Limited

Name: Mr Niclas Rosenlew

Authorised Signature DocuSigned by: N.R. 492EA66A566045E...

Date of signature 21-Mar-18

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
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 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 the Data Processing Appendix. Basware may modify its security measures from time to time but will not decrease the overall security during the term of the Data Processing Appendix.

DATA EXPORTER

Customer's signature of the main body of this DPA above applies.

DATA IMPORTER Basware India Private Limited

Name: Mr Niclas Rosenlew

Authorised Signature DocuSigned by: N. R. Rosenlew 492EA66A566045E...

Date of signature 21-Mar-18

ANNEX 2: BASWARE CLOUD SERVICES TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Prevent unauthorized persons from gaining access to data processing sites that process and use Personal Data (site access control)

Personal Data is processed and stored in professionally hosted data centres, which are protected with effective physical access control, including electronic locks, burglar alarms and CCTV monitoring. Only nominated, authorized persons have physical access to data centre facilities. All visitors are accompanied at all times.

Prevent data processing systems from being used without authorization (system access control)

Each user of data processing systems is authenticated with a personal user account. Shared or group accounts are not used for personal access. Each user account must be approved by a management sponsor, and each user is personally responsible for the user account and the ways in which it is used. User accounts are reviewed regularly, and unnecessary users are removed.

Ensure that persons authorized to use a data processing system have access only to the data they are authorized to access, and that Personal Data cannot be read, copied, modified, or removed without authorization during processing, use and storage (data access control)

Access rights to data processing systems are granted to pre-defined roles according to least privilege principle. Access to Personal Data must be justified with a clear and indisputable business need, and approved by a management sponsor. Special admin, etc. privileges are granted to an absolute minimum number of users. Access rights are reviewed regularly, and unnecessary rights are removed.

Ensure that Personal Data cannot be read, copied, modified, or removed without authorization during electronic transfer, or when saving to data storage media (transfer control)

Electronic transfers of Personal Data in public networks are encrypted. Transfers within a data centre environment may not be encrypted; however, access to networks and processing systems is strictly limited by site and system access control. It is forbidden to store Personal Data to removable media. Backups of Personal Data are encrypted.

Ascertain and check where and to whom Personal Data can be transferred by means of data transmission facilities (disclosure control)

Data flows of Personal Data are tracked to ensure comprehensive access control and to minimize the risk of accidental or unauthorized data disclosure. New connections and data transfers must be approved by a management sponsor. Transfer of Personal Data to non-production environments, such as testing, is forbidden without explicit customer approval and sufficient data masking.

Perform checks to establish whether and by whom Personal Data has been entered, modified, or removed in data processing system (input control)

Access to Personal Data is monitored, and an audit trail is created for all data processing systems. Access logs are stored in a separate, secure system, which prevents unauthorized modification or deletion of log events. Access logs are considered Personal Data, and are protected accordingly. Access logs are stored for a minimum of one (1) year, or for the minimum duration mandated by external compliance requirements.

Ensure that Personal Data processed on behalf of a customer is processed in strict accordance with the customer's instructions (order control)

The scope of Personal Data protection and how to deal with customer's instructions is further described in the Personal Data Processing Appendix.

Ensure that Personal Data is protected against accidental destruction or loss (availability control)

Personal Data is backed up at regular intervals. Copies of data backups are transferred securely to an offsite location for disaster recovery. Data processing systems and infrastructure utilize redundant technologies, and single points of failure are minimized. Recovery time and point objectives are determined, and every effort is made to adhere to them.

Ensure that data collected for different purposes can be processed separately (separation control)

Personal Data is processed in dedicated systems that are not shared with other services, applications or corporate entities. Within individual systems and databases, data is segregated with logical access control. Personal Data will not be used for different purposes other than what it has been collected for without explicit customer approval.

Ensure that the customer is notified promptly in the event of a material breach of any of the controls above (notification control)

Customers will receive a prompt notification in the event of a Personal Data breach, a significant security incident in data processing system, or a material deviation from any of the controls above. In case Personal Data is lost or compromised, customer will be invited to participate in incident resolution, and granted access to applicable logs.