Radware Global Data Processing Agreement (Customer)

This Global Data Processing Agreement ("**DPA**") is made and entered into by and between Radware ("**Processor**") and the counterparty to the Principal Agreement ("**Customer**" or "**Controller**").

This DPA forms an integral part of the written or electronic agreement and/or purchase documents, including, without limitation, any purchase orders and/or order confirmations, through which the Customer ordered and Radware has agreed to provide, the Service(s) (as amended from time to time, the "**Principal Agreement**").

By signing a hard copy of this DPA, or by accepting this DPA by electronic means or otherwise, or by receiving the Services from Radware, Customer enters this DPA on behalf of itself and in the name and on behalf of its Affiliates that are lawfully permitted to use Radware's Services. If Customer entered this DPA on behalf of a third-party controller, Customer represents and warrants to Processor that Customer's instructions in respect to the processing by Data Processor of Personal Data have been notified to, and authorized by, the third-party controller of Personal Data, in accordance with Customer's obligations under the Applicable Data Protection Laws.

This DPA reflects the parties' agreement with regard to the Processing of Personal Data in the performance by Radware, and the receipt by Customer, of the Service(s).

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

1.1.1 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the share of the stock, equity or voting interests of a party.

1.1.2 "Applicable Data Protection Laws" means, as the case may be, data protection laws addressing the safeguarding and lawful Processing of Personal Data that apply to the Services ordered by Customer, including the EU GDPR, the UK GDPR, and the CCPA.

1.1.3 "CCPA" means the California Consumer Privacy Act of 2018 Cal. Civil Code § 1798.100 et seq.

1.1.4 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data, and in the context of this DPA shall mean the Customer.

1.1.5 "Standard Contractual Clauses" or "SCC" means for personal data subject to the EU GDPR or the UK GDPR, as the context requires, the contractual clauses promulgated pursuant to the European Commission Implementation Decision (EU) 2021/914 of 4 June, 2021 on standard contractual clauses for the transfer of Personal Data to third countries, which do not ensure an adequate level of protection, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.1.6 "Customer Personal Data" means Personal Data described in Schedule A and any other Personal Data provided to Processor by or on behalf of Customer or by Customer's end users for Processing on behalf of the Customer pursuant to or in connection with the Principal Agreement.

1.1.7 "Data Subject" means an identified or identifiable natural person to whom Personal Data relates;

1.1.8 "DPA" means this Global Data Processing Agreement and all Schedules thereto.

1.1.9 "EEA" means the European Economic Area.

1.1.10 "EU GDPR" means EU General Data Protection Regulation 2016/679.

1.1.11 "Personal Data" means as the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined under Applicable Data Protection Laws.

1.1.12 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed by the Service.

1.1.13 "Processing" or "Process" means any operation or set of operations that is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, as described in the Principal Agreement and in Schedule A.

1.1.14 "Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of a Controller, and in the context of this DPA shall mean Radware.

1.1.15 "Radware" means Radware Ltd. or Radware Inc. depending on the Radware entity which is a party to the Principal Agreement.

1.1.16 "Services" means the services provided by Radware to Customer pursuant to the Principal Agreement.

1.1.17 "Subprocessor" means any third party appointed by Radware to Process Customer Personal Data on behalf of the Customer within the scope of and related to the Principal Agreement.

1.1.18 "Supervisory Authority" means an independent public authority which is established in a jurisdiction under Applicable Data Protection Laws with competence over matters pertaining to data protection.

1.1.19 "UK GDPR" means the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

2. Processing of Customer Personal Data

2.1 Processor shall not Process Customer Personal Data other than on the Customer's documented instructions including as described in Schedule A and in the Principal Agreement.

2.2 The Customer instructs Processor to process Customer Personal Data in accordance with Applicable Data Protection Laws: (a) to the extent required in order to carry out the Services pursuant to the Principal Agreement; (b) as further specified in the Data Processing Profile of the applicable Service attached hereto as **Schedule A**; (c) inputs into the Service Portal and other functionalities of the Services made through Customer's use of such Radware's computer systems; and (d) as further documented in any other written instructions given by Customer to Radware.

2.3 Customer acknowledges and agrees that:

2.3.1 Customer is (or is acting with full authority on behalf of) the "Controller" of any Customer Personal Data. Customer will comply with all legal requirements applicable to a Controller of Personal Data in connection with the Services and the Customer Personal Data.

2.3.2 Customer will (i) not disclose any Customer Personal Data or other Personal Data and information to Radware, nor shall Customer transmit or cause to be transmitted through the Service any Customer Personal Data or other Personal Data and information, if such disclosure or transmission would violate any applicable law including any Applicable Data Protection Laws, in

particular Customer shall ensure it has all necessary appropriate consents and notices in place to enable lawful transfer of and processing of Personal Data to Radware for the duration and purposes of the Principal Agreement; (ii) not request Radware to use, disclose or otherwise Process Customer Personal Data or other Personal Data and information in any manner that would violate any Applicable Data Protection Laws ; (iii) disclose to Radware or transmit or cause to be transmitted through the Services only the minimum amount of Customer Personal Data reasonably necessary for Radware to perform the Services under the Principal Agreement; and (iv) where practicable and commercially reasonable, de-identify and/or encrypt any such Customer Personal Data before making it available to Radware or before transmitting or cause to be transmitted such Customer Personal Data through the Services.

3.   Processor Personnel

Processor shall take reasonable steps to provide the reliability of any employee, agent or contractor of Processor who may have access to the Customer Personal Data, providing in each case that access is strictly limited to those individuals who need to know and/or access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Data Protection Laws in the context of that individual's duties to the Processor, providing that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4.   Security

4.1   Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures designed to provide a level of security appropriate to that risk in the provision of the Services, including, if applicable and as appropriate, in consistent with the measures as referred to in Article 32(1) of the GDPR, and as set forth in **Schedule B**.

4.2   In assessing the appropriate level of security, Processor shall take into account in particular the risks that are presented by Processing, in particular from a Personal Data Breach.

5.   Subprocessing

5.1   Except as set forth is section 5.3 below, Processor shall not appoint (or disclose any Customer Personal Data to) any Subprocessor unless required or authorized by the Customer.

5.2   With respect to each Subprocessor, Radware will impose substantially similar data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor Processing any Customer Personal Data. As between the Customer and Radware, Radware shall remain liable for all acts or omissions of any Subprocessor appointed by it pursuant to this section 5.2 and section 5.3 below.

5.3   The Customer acknowledges and agrees that Radware uses the Subprocessors set out in **Schedule C** and as described in **Schedule A**, for the purpose of Processing data in connection with the Services including for the purpose of Processing Customer Personal Data; provided that Radware reserves the right to update the list of Subprocessors in **Schedule C** by providing a notice in writing to Customer, and such updated list shall be deemed accepted by Customer unless Customer raises an objection in writing within thirty (30) days of receipt of such notice. The Customer acknowledges that where it raises an objection to the use of a Subprocessor its use of the Service under the Principal Agreement may be limited or impossible and Processor shall have no liability in respect of any such limitation or impossibility. Customer's sole recourse if Customer objects to the appointment of a new Subprocessor will be to terminate the Principal Agreement with regard to the affected Service by providing Radware with written notice within thirty (30) days of receipt of the notice informing Customer of a change in the list of Subprocessors.

6.   Data Subject Rights

6.1   Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under Appliable Data Protection Laws.

6.2   Processor shall:

6.2.1   Promptly notify Customer if it receives a request from a Data Subject under Applicable Data Protection Law in respect of Customer Personal Data; and

6.2.2   Not respond to that request except on the documented instructions of Customer or as required by Applicable Data Protection Law to which the Processor is subject, in which case Processor shall, to the extent permitted by Appliable Data Protection Laws, inform Customer of that legal requirement before the Processor responds to the request.

7.   Personal Data Breach

7.1   Processor shall notify Customer without undue delay within 72 hours upon Processor becoming aware of a Personal Data Breach, thereby providing Customer with sufficient

information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Applicable Data Protection Laws.

7.2   Processor shall reasonably co-operate with the Customer and take reasonable commercial steps as are reasonably directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8.   Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Applicable Data Protection Laws (including article 35 or 36 of the GDPR to the extent applicable), in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Processor. To the extent that any such impact assessment and/or prior consultation requires assistance beyond Radware providing the applicable Radware processing record(s) and documentation, Radware reserves the right to charge Customer for such engagement at Radware's then current daily rates.

9.   Deletion or return of Customer Personal Data

9.1   Subject to this section 9, Processor shall, as soon as reasonably feasible after the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), but, in any event, in accordance with Applicable Data Protection Laws, delete and procure the deletion of all copies of those Customer Personal Data.

9.2   Upon Customer's request, Processor shall provide written confirmation to Customer that it has fully complied with this section 9 within ten (10) business days of the Cessation Date.

10.   Information and Audit Rights

10.1   The Processor maintains industry security standard certifications for cybersecurity and privacy, issued by an independent third-party auditor, further information can be found at https://www.radware.com/newsroom/certifications/. The Processor will continue to undergo annual audits necessary for maintaining such certifications for the Services during the term of the Principal Agreement. Moreover, an annual Service Organization Control 2 (SOC 2) Type II Report is being prepared for Radware's cloud Services and in addition Radware relies on the SOC 2 Type II audits undergone by some of its Subprocessors. Subject to the Processor's confidentiality obligations and upon request, the Processor will provide the Customer with a copy of the most recent SOC 2 Type II Report(s) and/or excerpt of any of Processor's available SOC 2 Type II Report and such Reports of its Subprocessors upon written request by the Customer.

The Customer agrees that the Processor's obligations set forth in this section 10.1 fully satisfy the information and audit rights under Applicable Data Protection Laws, including under Article 28.3(h) of the EU GDPR as well as under Clause 8.9 and Clause 13(b) of the SCC.

10.2   The audit rights of the Customer under section 10.1 above are without derogating from any audit rights provided under the Principal Agreement (if any).

11.   Onward and Trans-Border Data Transfer

11.1.   Transfer of GDPR-governed Customer's Personal Data ("**EEA Transferred Data**") to a Third Country, is made in accordance with the EU Standard Contractual Clauses ("**EU SCCs**"), pursuant to EU Commission Decision C(2021)3972, giving effect to the module specified in __Exhibit A__ which is attached and incorporated by reference to this DPA, or, as required, in accordance with any successor thereof or an alternative lawful data transfer mechanism, and as follows:

11.1.1.   In Clause 7, the optional docking clause will apply;

11.1.2.   If applicable - in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes will be as set out in Section 5 of this DPA;

11.1.3.   In Clause 11, the optional language will not apply;

11.1.4.   In Clause 17, Option 1 will apply, and the EU SCCs will be governed by the Irish law;

11.1.5.   In clause 18(b), disputes will be resolved before the courts of Ireland.

11.2.   In accordance with Article 46 of the GDPR and the EU SCCs, and without prejudice to any provisions of this DPA, Processor undertakes to implement the following organizational and technical safeguards, in addition to the safeguards mandated by the EU SCCs and in accordance with Clause 14(b)(iii) of the EU SCCs, to ensure the required adequate level of protection to the EEA Transferred Data:

11.2.1.   Processor will implement and maintain the technical measures, as specified in Annex II of Exhibit A, which is attached and incorporated by reference to this DPA, with a purpose to protect the EEA Transferred Data from Processing for national security or other governmental purposes that goes beyond what is necessary and proportionate in a democratic society, considering the type of Processing activities under the Agreement and relevant circumstances;

11.2.2.   For the purposes of safeguarding EEA Transferred Data when any Third Country's government or regulatory agency requests access to such data

("**Request**"), and unless required by a valid court order or if otherwise Processor may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to EEA Transferred Data, or where the access is requested in the event of imminent threat to lives, Processor will:

11.2.2.1. not purposefully create 'back doors' or similar programming that could be used to access the EEA Transferred Data;

11.2.2.2. not provide the source code or encryption keys to any government agency for the purpose of accessing the EEA Transferred Data; and

11.2.2.3. upon Customer's written request, provide reasonable available information about the requests of access to Personal Data by government agencies that Processor has received in the six (6) months preceding to Customer's request.

11.2.3. If Processor receives a Request, Processor will notify Customer of such request to enable the Customer to take necessary actions, to communicate directly with the relevant agency and to respond to the Request. If Processor is prohibited by law to notify the Customer of the Request, Processor will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer's expense and, to the extent possible, will provide only the minimum amount of information necessary.

11.3. Transfer of UK GDPR-governed Customer's Personal Data ("**UK Transferred Data**") to a Third Country, is either:

11.3.1 made in accordance with the International Data Transfer Agreement ("**IDTA**"), issued by the Information Commissioner's Office's ("**ICO**") in accordance with section 119A of the Data Protection Act 2018, as officially published at: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf;

OR

11.3.2 made in accordance with the UK Addendum issued by the ICO in accordance with section 119A(1) of the Data Protection Act 2018 ("**UK Addendum**"), incorporating EU SCCs (officially published at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

12.   General Terms

12.1   This DPA is without prejudice to the rights and obligations of the parties under the Principal Agreement which shall continue to have full force and effect. Any claims brought under this DPA shall be subject to the terms of the Principal Agreement including, without limitation, choice of jurisdiction, governing law and any liability limitations or exclusions. In the event of any conflict between the terms of this DPA and the terms of the Principal Agreement and/or any other agreements between the parties, including (except where explicitly agreed otherwise in writing and signed on behalf of the parties) agreements entered into or purported to be entered into after the date signing or acceptance of this DPA, the terms of this DPA shall prevail but only so far as the subject matter concerns the processing of Personal Data.

In the event of any conflict or inconsistency between this DPA or the Principal Agreement and the SCC, the latter shall prevail.

12.2   Radware's liability under or in connection with this DPA is subject to the limitations on liability contained in the Principal Agreement.

12.3   In the event the Principal Agreement does not include limitations of liability, the following limitations of liability will apply between the parties in connection with this DPA including with regards to the applicable Standard Contractual Clauses:

Neither party shall be liable to the other party or to any third party, for any special, indirect, incidental or consequential, exemplary or reliance damages, losses or expenses (including without limitation, loss of profits, loss of information, loss or corruption of data, loss or interruption of business) arising from or in any way connected with the parties' obligations under this DPA, however caused, and whether based on contract, tort (including negligence), equity or other theory of liability whatsoever, even if such party has been advised of the possibility of such damages or losses or expenses. Without derogating from the foregoing, except for liability for payments for the Services, in no event shall a party's total aggregate liability to the other party exceed the amounts actually paid to Supplier for the Service that is the subject matter of the claim during the twelve (12) month period preceding the damaging event. This section will survive the termination/expiration any sale/purchase document between Radware and Customer. Notwithstanding the foregoing, none of the exclusions and limitations in this section shall apply in respect of (i) liability in negligence causing personal injury or death; (ii) liability for fraudulent misrepresentation; or (iii) any other liability which cannot by law be excluded or limited (as appropriate).

12.4   In the event the Principal Agreement does not include a provision addressing governing law and jurisdiction, the following will apply between the parties in connection with this

DPA: the DPA will be governed and construed in accordance with the substantive laws of, and exclusive venue will be located in: (i) Israel if Customer is located in Israel; (ii) England and Wales if Customer is located in EMEA; (iii) Singapore if Purchaser is located in APAC; and (iv) the state of New York for all other Customer locations.

12.5 The applicable law provisions of this DPA are without prejudice to clauses 17 (Governing law) and Clause 18 (Choice of forum and jurisdiction) of the SCC where applicable to transfers of Personal Data from the EEA or the UK to a third country.

12.6 To the extent that Processing relates to Personal Data originating from a jurisdiction or Processed in a jurisdiction which has any mandatory requirements in addition to those that are set out in this DPA, Customer will inform Radware of such additional mandatory requirements and both parties may agree to any additional measures required to provide compliance with such applicable additional mandatory requirements and any such additional measures agreed to by the parties will be documented as an Annex to this DPA or in an Order under the Principal Agreement. Due to the fact that Radware has no control over the type, character, properties, content, and/or origin of Customer Personal Data Processed hereunder, notwithstanding anything to the contrary herein, Radware shall not be in breach of this DPA or the Principal Agreement or liable to Customer to the extent Customer Personal Data subject to jurisdictional requirements mandating security, processing or other measures not set forth in, or contrary to the terms of, this DPA is provided by Customer without first informing Radware and amending this DPA or entering into an Order addressing the same.

12.7 If any variation is required to this DPA as a result of a change in Applicable Data Protection Laws, including any variation which is required to the data export mechanism (including any new or successor version of the SCC) for the transfer of Personal Data not described in this DPA ("Alternative Transfer Mechanism"), then either party may provide written notice to the other party of that change in law. The Parties will discuss and negotiate in good faith any necessary variations to this DPA, including the Standard Contractual Clauses, to address such changes, and Customer agrees to execute such other and further documents to give legal effect to such Alternative Transfer Mechanism, to the extent such Alternative Transfer Mechanism complies with the Applicable Data Protection Laws in the territories to which Personal Data is transferred.

12.8 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be: (i) amended as necessary to ensure its validity and enforceability while preserving the parties' intentions as closely as possible, or, if this is not possible; (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12.9 To the maximum extent legally permitted, there are no third-party beneficiaries under this DPA.

North America
Radware Inc.
575 Corporate Drive
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 6971917, Israel
Tel: 972 3 766 8666

SCHEDULE A
DATA PROCESSING ACTIVITY PROFILE

CWAF Data Processing Profile
CDDOS Data Processing Profile
BOTM Data Processing Profile
CNP Data Processing Profile

SCHEDULE B -
TECHNICAL AND ORGANISATIONAL SECURITY MEASURES
<u>**Also serves as Annex II to the EU SCC**</u>

Processor shall implement appropriate technical and organizational security measures intended to protect the Customer Personal Data it Processes against accidental or unauthorized loss, destruction, alteration, disclosure or access:

IS Program - Radware maintains an information security program with the aim to identify reasonably foreseeable external and internal risks to the security of Radware Network and minimize security risks through risk assessments and regular testing.

CISO - Radware has designated a Chief Information Security Officer (CISO) to coordinate and be accountable for the information security management system.

Baseline for the Security and Privacy Management System - Radware follows industry best practices for its Information Security Management system (ISMS) and Privacy Management System(PIMS). Radware's compliance with these standards is certified annually for ISO 27001, ISO 27017, ISO 27018, ISO 27032 and ISO 27701.

PCI Service Provider (where appropriate) and HIPAA compliance is confirmed by an annual self-assessment process.

Security Reviews - Radware conducts periodic reviews of the security of its infrastructure and the adequacy of its information security program. Evidence of these reviews include annual SOC2 Type II reports prepared by a qualified 3rd party.

Human Resources - Radware provides that employees, contractors, partners, and vendors understand their data protection and security responsibilities. These responsibilities include maintaining the confidentiality, integrity and availability of the Customer information processed by Radware. All employees of the organization and where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Access Control

Radware provides that only authorized users will have access to its information assets and to private data. Users are only be provided with access to assets that they have been specifically authorized to use.

Radware provides the customers with an access control management system for the relevant cloud management portals as part of the service.

Encryption - Radware provides proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, Radware will provide that confidential data will be encrypted whenever extracted from their primary repository.

Physical and Environmental Security - Radware will use physical and environmental measures to prevent unauthorized physical access, damage to or disruption of the organization's information and information processing facilities.

Operational & Communication Security - Radware will maintain appropriate controls related to management of IT production including change management, capacity management, malware, backup, logging, monitoring and vulnerabilities management.

System acquisition, development, and maintenance - Radware maintains security throughout the lifecycle of the information systems.

Supplier Relationship - Radware provides that its partners, suppliers, and contractors maintain adequate security measurements to secure Radware and its customers' information, through contracts and periodic audits.

Data Retention and disposal

Information stored withing the service, such as logs and alerts will be retained according to customer requirements. When no longer required, the information will be securely deleted or destroyed.

SCHEDULE C
LIST OF CURRENT SUB-PROCESSORS
Also serves as Annex III to the EU SCC

[Radware Cloud Services Sub-Processors List](#)

SCHEDULE D

Standard Contractual Clauses

ANNEX to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as officially published at:
https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf or other official publications of the European Union as updated from time to time:

☐ **MODULE TWO: Transfer controller to processor**

☐ **MODULE THREE: Transfer processor to processor**

[Tick the box next to the relevant transfer module]

APPENDIX

ANNEX I

Also serves as Annex I to the EU SCC

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …Unitisation of the Radware Cloud services and/or support services ordered from the Data Importer pursuant to the Principle Agreement

Signature and date: …

Role (controller/processor): …Controller

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: … **Radware Ltd and its Affilate**

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …Provision of the Cloud Services and/or support services ordered by the Data Exporter pursuan to the Principle Agreement

Signature and date: …

Role (controller/processor): …Processor

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As specifiend in the Data Profile Document of the Radware products and services used by the Data Exporter(s) at the links availaible in Schedual A

Categories of personal data transferred

As specifiend in the Data Profile Document of the Radware cloud products and services used by the Data Exporter(s) at the links availaible at Schedual A

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not Applicalbe unless otherwies specifiy in the Data Proflie Doducments abvoe………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Information is transferred on an ongoing basis depending on the level of services ordered by the Data Exporter; one-off basis for supprot requests …………………………

Nature of the processing

Processing necessary to provide the Services to Customer pursuant to the Agreement; See Schedule A

Purpose(s) of the data transfer and further processing

Processing necessary to provide the Services to Customer pursuant to the Agreement; See Schedule A

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As specified in Schedule A for the product and services utilised by the Data Exporter

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As specified in Schedule A

C. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter is established in an EU Member State - the supervisory authority of such EU Member State shall act as competent supervisory authority

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the supervisory authority of the Member State in which the representative is established shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) - the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.