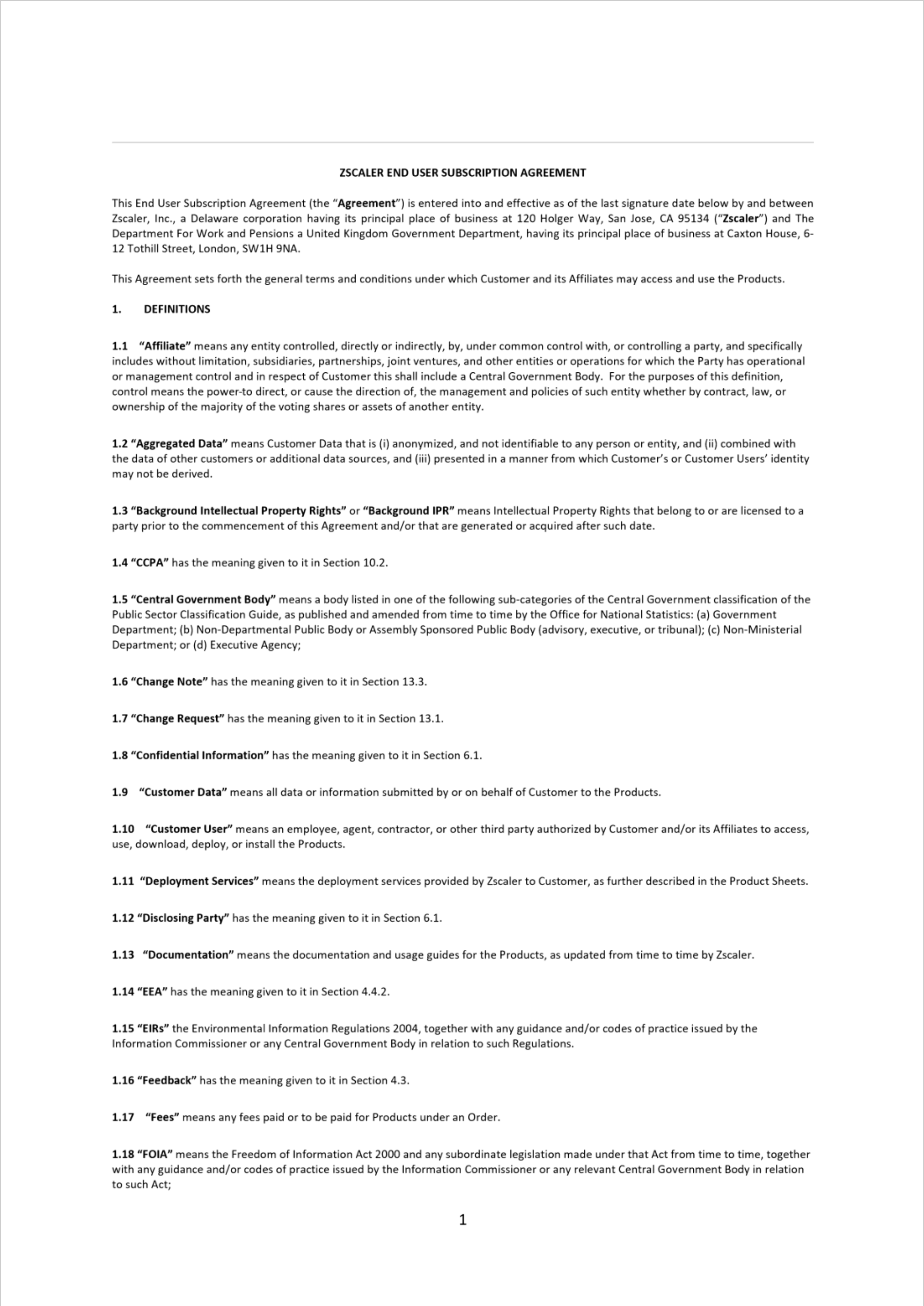
DWP EUSA FINAL_Redacted ZScaler

30 June 2020 14:47

DWP EUSA FINAL_Redacted ZScaler



ZSCALER END USER SUBSCRIPTION AGREEMENT

This End User Subscription Agreement (the "**Agreement**") is entered into and effective as of the last signature date below by and between Zscaler, Inc., a Delaware corporation having its principal place of business at 120 Holger Way, San Jose, CA 95134 ("**Zscaler**") and The Department For Work and Pensions a United Kingdom Government Department, having its principal place of business at Caxton House, 6-12 Tothill Street, London, SW1H 9NA.

This Agreement sets forth the general terms and conditions under which Customer and its Affiliates may access and use the Products.

1. DEFINITIONS

1.1 "Affiliate" means any entity controlled, directly or indirectly, by, under common control with, or controlling a party, and specifically includes without limitation, subsidiaries, partnerships, joint ventures, and other entities or operations for which the Party has operational or management control and in respect of Customer this shall include a Central Government Body. For the purposes of this definition, control means the power-to direct, or cause the direction of, the management and policies of such entity whether by contract, law, or ownership of the majority of the voting shares or assets of another entity.

1.2 "Aggregated Data" means Customer Data that is (i) anonymized, and not identifiable to any person or entity, and (ii) combined with the data of other customers or additional data sources, and (iii) presented in a manner from which Customer's or Customer Users' identity may not be derived.

1.3 "Background Intellectual Property Rights" or **"Background IPR"** means Intellectual Property Rights that belong to or are licensed to a party prior to the commencement of this Agreement and/or that are generated or acquired after such date.

1.4 "CCPA" has the meaning given to it in Section 10.2.

1.5 "Central Government Body" means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;

1.6 "Change Note" has the meaning given to it in Section 13.3.

1.7 "Change Request" has the meaning given to it in Section 13.1.

1.8 "Confidential Information" has the meaning given to it in Section 6.1.

1.9 "Customer Data" means all data or information submitted by or on behalf of Customer to the Products.

1.10 "Customer User" means an employee, agent, contractor, or other third party authorized by Customer and/or its Affiliates to access, use, download, deploy, or install the Products.

1.11 "Deployment Services" means the deployment services provided by Zscaler to Customer, as further described in the Product Sheets.

1.12 "Disclosing Party" has the meaning given to it in Section 6.1.

1.13 "Documentation" means the documentation and usage guides for the Products, as updated from time to time by Zscaler.

1.14 "EEA" has the meaning given to it in Section 4.4.2.

1.15 "EIRs" the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Central Government Body in relation to such Regulations.

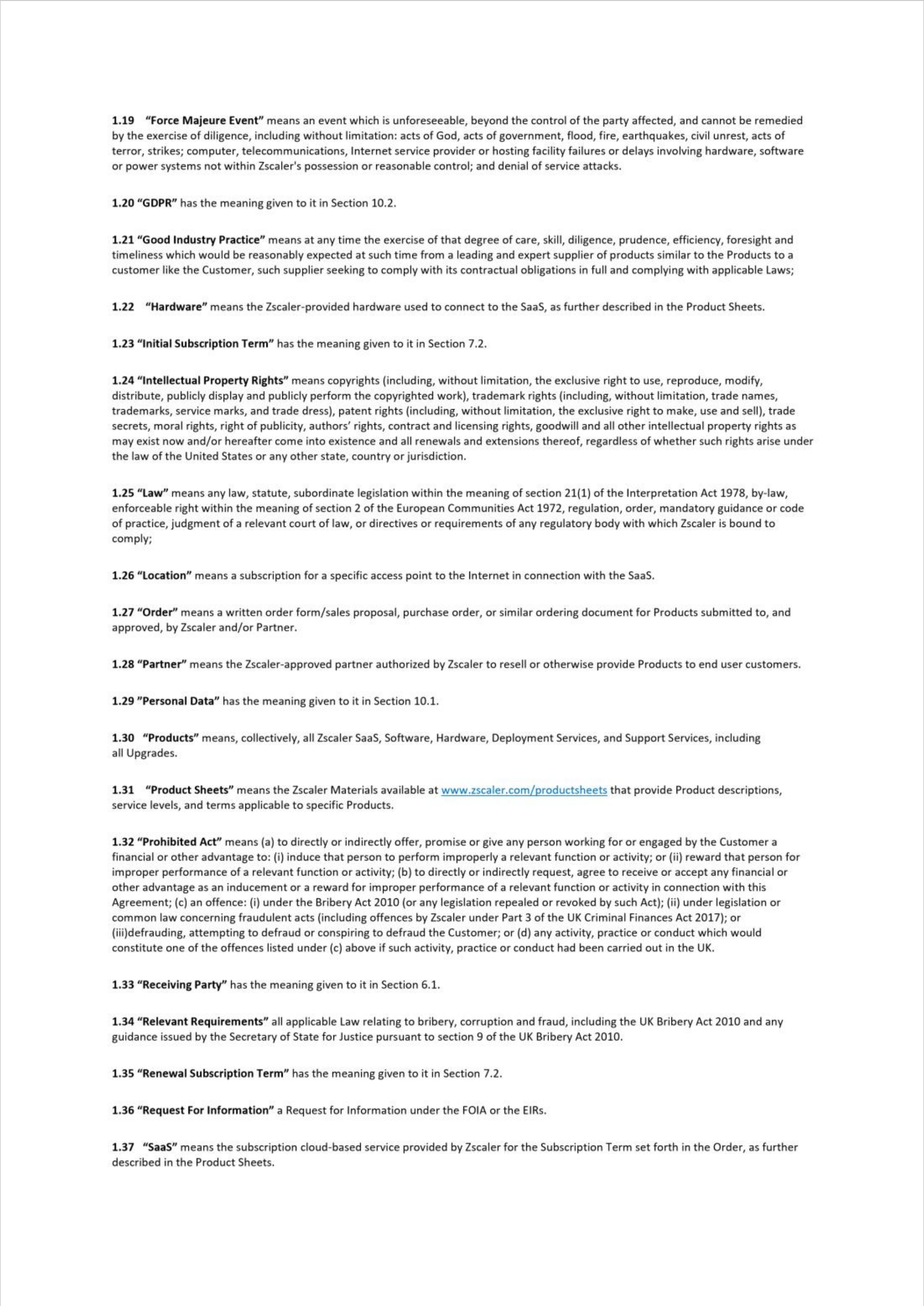
1.16 "Feedback" has the meaning given to it in Section 4.3.

1.17 "Fees" means any fees paid or to be paid for Products under an Order.

1.18 "FOIA" means the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Central Government Body in relation to such Act;

Page 2

30 June 2020 14:55



1.19 "Force Majeure Event" means an event which is unforeseeable, beyond the control of the party affected, and cannot be remedied by the exercise of diligence, including without limitation: acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes; computer, telecommunications, Internet service provider or hosting facility failures or delays involving hardware, software or power systems not within Zscaler's possession or reasonable control; and denial of service attacks.

1.20 "GDPR" has the meaning given to it in Section 10.2.

1.21 "Good Industry Practice" means at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of products similar to the Products to a customer like the Customer, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws;

1.22 "Hardware" means the Zscaler-provided hardware used to connect to the SaaS, as further described in the Product Sheets.

1.23 "Initial Subscription Term" has the meaning given to it in Section 7.2.

1.24 "Intellectual Property Rights" means copyrights (including, without limitation, the exclusive right to use, reproduce, modify, distribute, publicly display and publicly perform the copyrighted work), trademark rights (including, without limitation, trade names, trademarks, service marks, and trade dress), patent rights (including, without limitation, the exclusive right to make, use and sell), trade secrets, moral rights, right of publicity, authors' rights, contract and licensing rights, goodwill and all other intellectual property rights as may exist now and/or hereafter come into existence and all renewals and extensions thereof, regardless of whether such rights arise under the law of the United States or any other state, country or jurisdiction.

1.25 "Law" means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, by-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which Zscaler is bound to comply;

1.26 "Location" means a subscription for a specific access point to the Internet in connection with the SaaS.

1.27 "Order" means a written order form/sales proposal, purchase order, or similar ordering document for Products submitted to, and approved, by Zscaler and/or Partner.

1.28 "Partner" means the Zscaler-approved partner authorized by Zscaler to resell or otherwise provide Products to end user customers.

1.29 "Personal Data" has the meaning given to it in Section 10.1.

1.30 "Products" means, collectively, all Zscaler SaaS, Software, Hardware, Deployment Services, and Support Services, including all Upgrades.

1.31 "Product Sheets" means the Zscaler Materials available at www.zscaler.com/productsheets that provide Product descriptions, service levels, and terms applicable to specific Products.

1.32 "Prohibited Act" means (a) to directly or indirectly offer, promise or give any person working for or engaged by the Customer a financial or other advantage to: (i) induce that person to perform improperly a relevant function or activity; or (ii) reward that person for improper performance of a relevant function or activity; (b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Agreement; (c) an offence: (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); (ii) under legislation or common law concerning fraudulent acts (including offences by Zscaler under Part 3 of the UK Criminal Finances Act 2017); or (iii)defrauding, attempting to defraud or conspiring to defraud the Customer; or (d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK.

1.33 "Receiving Party" has the meaning given to it in Section 6.1.

1.34 "Relevant Requirements" all applicable Law relating to bribery, corruption and fraud, including the UK Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the UK Bribery Act 2010.

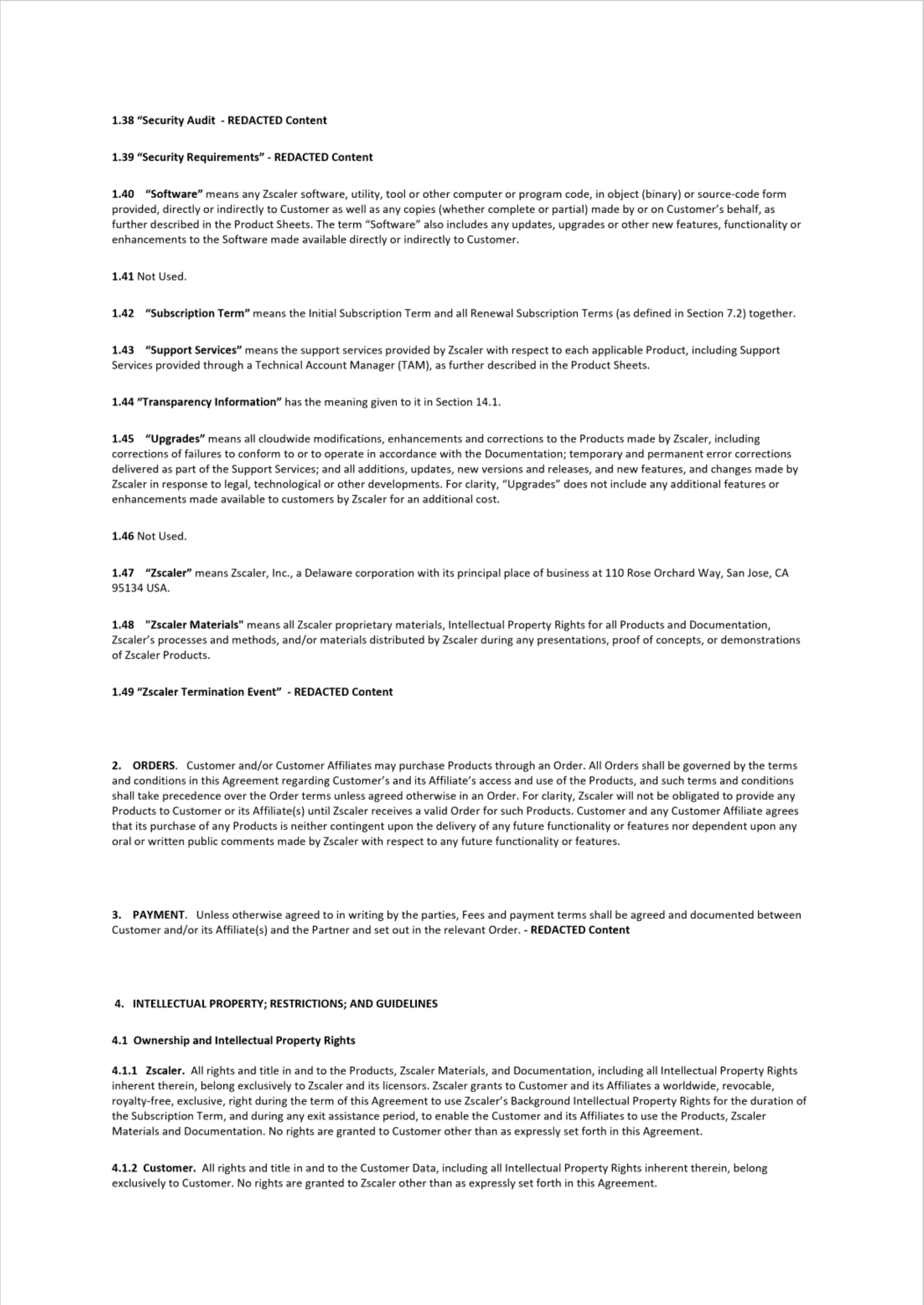
1.35 "Renewal Subscription Term" has the meaning given to it in Section 7.2.

1.36 "Request For Information" a Request for Information under the FOIA or the EIRs.

1.37 "SaaS" means the subscription cloud-based service provided by Zscaler for the Subscription Term set forth in the Order, as further described in the Product Sheets.

Page 3

30 June 2020 14:55



1.38 “Security Audit - REDACTED Content

1.39 “Security Requirements” - REDACTED Content

1.40 “Software” means any Zscaler software, utility, tool or other computer or program code, in object (binary) or source-code form provided, directly or indirectly to Customer as well as any copies (whether complete or partial) made by or on Customer’s behalf, as further described in the Product Sheets. The term “Software” also includes any updates, upgrades or other new features, functionality or enhancements to the Software made available directly or indirectly to Customer.

1.41 Not Used.

1.42 “Subscription Term” means the Initial Subscription Term and all Renewal Subscription Terms (as defined in Section 7.2) together.

1.43 “Support Services” means the support services provided by Zscaler with respect to each applicable Product, including Support Services provided through a Technical Account Manager (TAM), as further described in the Product Sheets.

1.44 “Transparency Information” has the meaning given to it in Section 14.1.

1.45 “Upgrades” means all cloudwide modifications, enhancements and corrections to the Products made by Zscaler, including corrections of failures to conform to or to operate in accordance with the Documentation; temporary and permanent error corrections delivered as part of the Support Services; and all additions, updates, new versions and releases, and new features, and changes made by Zscaler in response to legal, technological or other developments. For clarity, “Upgrades” does not include any additional features or enhancements made available to customers by Zscaler for an additional cost.

1.46 Not Used.

1.47 “Zscaler” means Zscaler, Inc., a Delaware corporation with its principal place of business at 110 Rose Orchard Way, San Jose, CA 95134 USA.

1.48 "Zscaler Materials" means all Zscaler proprietary materials, Intellectual Property Rights for all Products and Documentation, Zscaler’s processes and methods, and/or materials distributed by Zscaler during any presentations, proof of concepts, or demonstrations of Zscaler Products.

1.49 “Zscaler Termination Event” - REDACTED Content

2. ORDERS. Customer and/or Customer Affiliates may purchase Products through an Order. All Orders shall be governed by the terms and conditions in this Agreement regarding Customer’s and its Affiliate’s access and use of the Products, and such terms and conditions shall take precedence over the Order terms unless agreed otherwise in an Order. For clarity, Zscaler will not be obligated to provide any Products to Customer or its Affiliate(s) until Zscaler receives a valid Order for such Products. Customer and any Customer Affiliate agrees that its purchase of any Products is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written public comments made by Zscaler with respect to any future functionality or features.

3. PAYMENT. Unless otherwise agreed to in writing by the parties, Fees and payment terms shall be agreed and documented between Customer and/or its Affiliate(s) and the Partner and set out in the relevant Order. **- REDACTED Content**

4. INTELLECTUAL PROPERTY; RESTRICTIONS; AND GUIDELINES

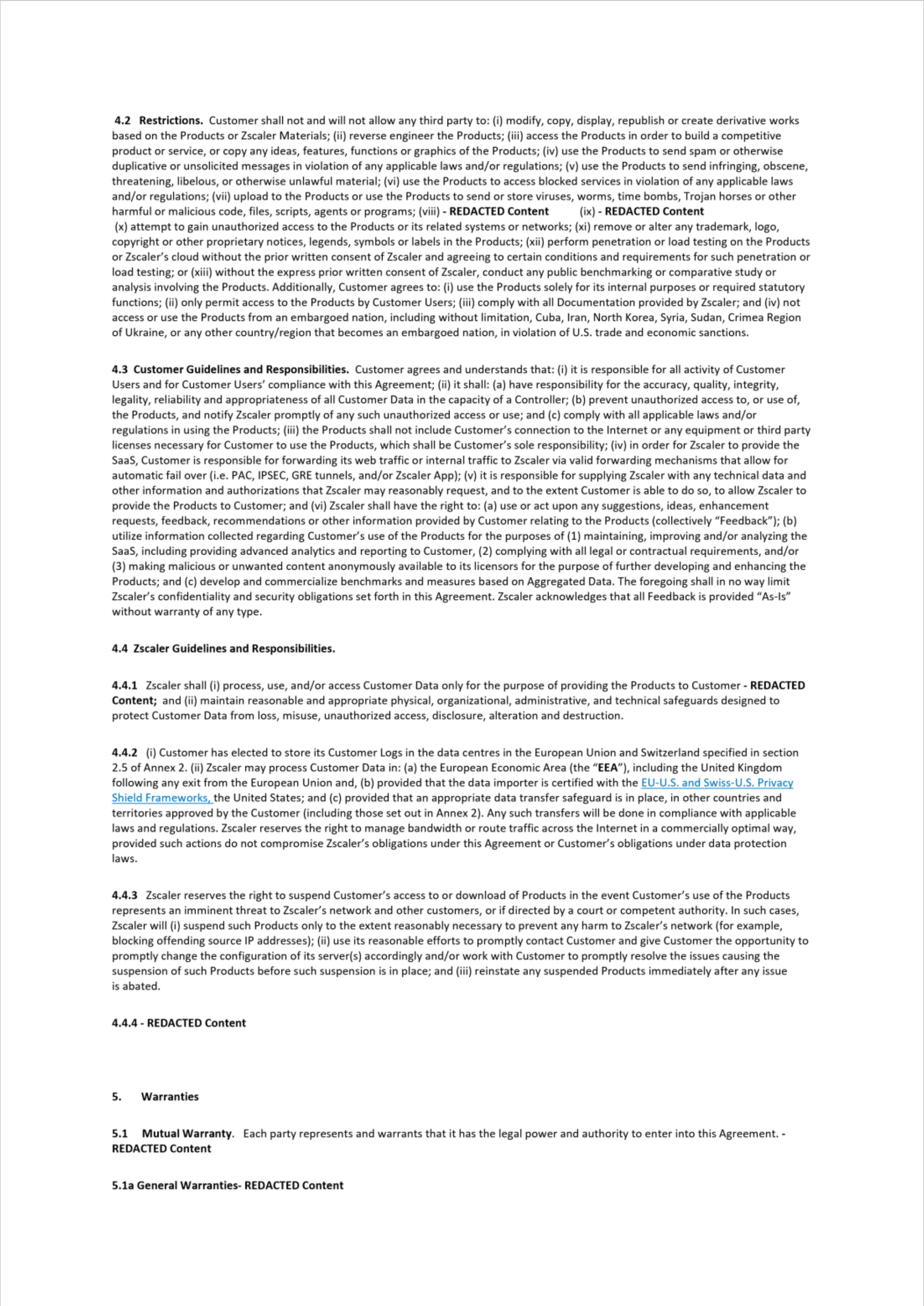
4.1 Ownership and Intellectual Property Rights

4.1.1 Zscaler. All rights and title in and to the Products, Zscaler Materials, and Documentation, including all Intellectual Property Rights inherent therein, belong exclusively to Zscaler and its licensors. Zscaler grants to Customer and its Affiliates a worldwide, revocable, royalty-free, exclusive, right during the term of this Agreement to use Zscaler’s Background Intellectual Property Rights for the duration of the Subscription Term, and during any exit assistance period, to enable the Customer and its Affiliates to use the Products, Zscaler Materials and Documentation. No rights are granted to Customer other than as expressly set forth in this Agreement.

4.1.2 Customer. All rights and title in and to the Customer Data, including all Intellectual Property Rights inherent therein, belong exclusively to Customer. No rights are granted to Zscaler other than as expressly set forth in this Agreement.

Page 4

30 June 2020 14:55



4.2 Restrictions. Customer shall not and will not allow any third party to: (i) modify, copy, display, republish or create derivative works based on the Products or Zscaler Materials; (ii) reverse engineer the Products; (iii) access the Products in order to build a competitive product or service, or copy any ideas, features, functions or graphics of the Products; (iv) use the Products to send spam or otherwise duplicative or unsolicited messages in violation of any applicable laws and/or regulations; (v) use the Products to send infringing, obscene, threatening, libelous, or otherwise unlawful material; (vi) use the Products to access blocked services in violation of any applicable laws and/or regulations; (vii) upload to the Products or use the Products to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs; (viii) **- REDACTED Content** (ix) **- REDACTED Content** (x) attempt to gain unauthorized access to the Products or its related systems or networks; (xi) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Products; (xii) perform penetration or load testing on the Products or Zscaler's cloud without the prior written consent of Zscaler and agreeing to certain conditions and requirements for such penetration or load testing; or (xiii) without the express prior written consent of Zscaler, conduct any public benchmarking or comparative study or analysis involving the Products. Additionally, Customer agrees to: (i) use the Products solely for its internal purposes or required statutory functions; (ii) only permit access to the Products by Customer Users; (iii) comply with all Documentation provided by Zscaler; and (iv) not access or use the Products from an embargoed nation, including without limitation, Cuba, Iran, North Korea, Syria, Sudan, Crimea Region of Ukraine, or any other country/region that becomes an embargoed nation, in violation of U.S. trade and economic sanctions.

4.3 Customer Guidelines and Responsibilities. Customer agrees and understands that: (i) it is responsible for all activity of Customer Users and for Customer Users' compliance with this Agreement; (ii) it shall: (a) have responsibility for the accuracy, quality, integrity, legality, reliability and appropriateness of all Customer Data in the capacity of a Controller; (b) prevent unauthorized access to, or use of, the Products, and notify Zscaler promptly of any such unauthorized access or use; and (c) comply with all applicable laws and/or regulations in using the Products; (iii) the Products shall not include Customer's connection to the Internet or any equipment or third party licenses necessary for Customer to use the Products, which shall be Customer's sole responsibility; (iv) in order for Zscaler to provide the SaaS, Customer is responsible for forwarding its web traffic or internal traffic to Zscaler via valid forwarding mechanisms that allow for automatic fail over (i.e. PAC, IPSEC, GRE tunnels, and/or Zscaler App); (v) it is responsible for supplying Zscaler with any technical data and other information and authorizations that Zscaler may reasonably request, and to the extent Customer is able to do so, to allow Zscaler to provide the Products to Customer; and (vi) Zscaler shall have the right to: (a) use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer relating to the Products (collectively "Feedback"); (b) utilize information collected regarding Customer's use of the Products for the purposes of (1) maintaining, improving and/or analyzing the SaaS, including providing advanced analytics and reporting to Customer, (2) complying with all legal or contractual requirements, and/or (3) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Products; and (c) develop and commercialize benchmarks and measures based on Aggregated Data. The foregoing shall in no way limit Zscaler's confidentiality and security obligations set forth in this Agreement. Zscaler acknowledges that all Feedback is provided "As-Is" without warranty of any type.

4.4 Zscaler Guidelines and Responsibilities.

4.4.1 Zscaler shall (i) process, use, and/or access Customer Data only for the purpose of providing the Products to Customer **- REDACTED Content;** and (ii) maintain reasonable and appropriate physical, organizational, administrative, and technical safeguards designed to protect Customer Data from loss, misuse, unauthorized access, disclosure, alteration and destruction.

4.4.2 (i) Customer has elected to store its Customer Logs in the data centres in the European Union and Switzerland specified in section 2.5 of Annex 2. (ii) Zscaler may process Customer Data in: (a) the European Economic Area (the "**EEA**"), including the United Kingdom following any exit from the European Union and, (b) provided that the data importer is certified with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, the United States; and (c) provided that an appropriate data transfer safeguard is in place, in other countries and territories approved by the Customer (including those set out in Annex 2). Any such transfers will be done in compliance with applicable laws and regulations. Zscaler reserves the right to manage bandwidth or route traffic across the Internet in a commercially optimal way, provided such actions do not compromise Zscaler's obligations under this Agreement or Customer's obligations under data protection laws.

4.4.3 Zscaler reserves the right to suspend Customer's access to or download of Products in the event Customer's use of the Products represents an imminent threat to Zscaler's network and other customers, or if directed by a court or competent authority. In such cases, Zscaler will (i) suspend such Products only to the extent reasonably necessary to prevent any harm to Zscaler's network (for example, blocking offending source IP addresses); (ii) use its reasonable efforts to promptly contact Customer and give Customer the opportunity to promptly change the configuration of its server(s) accordingly and/or work with Customer to promptly resolve the issues causing the suspension of such Products before such suspension is in place; and (iii) reinstate any suspended Products immediately after any issue is abated.

4.4.4 - REDACTED Content

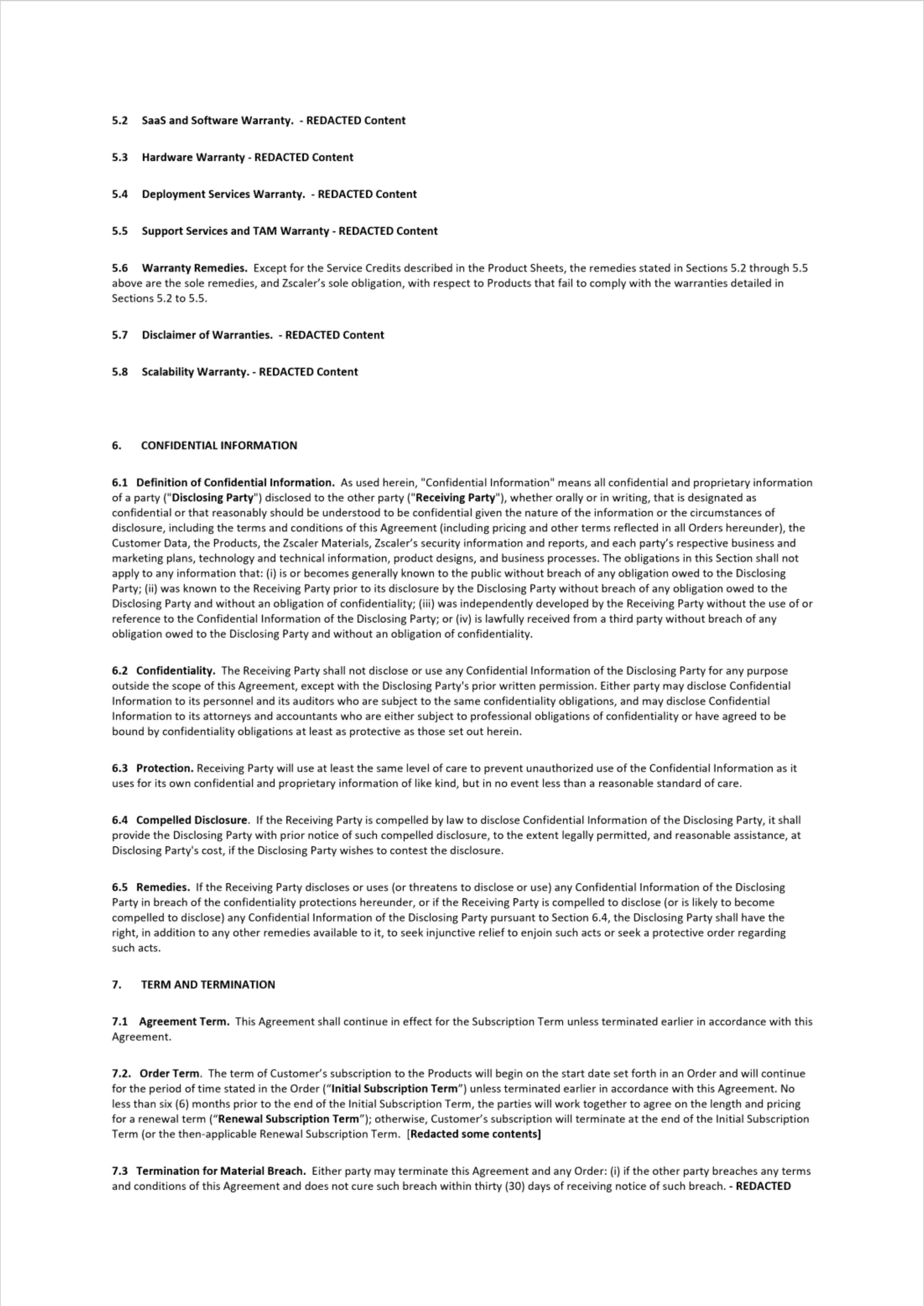
5. Warranties

5.1 Mutual Warranty. Each party represents and warrants that it has the legal power and authority to enter into this Agreement. **- REDACTED Content**

5.1a General Warranties- REDACTED Content

Page 5

30 June 2020 14:55



5.2 SaaS and Software Warranty. - REDACTED Content

5.3 Hardware Warranty - REDACTED Content

5.4 Deployment Services Warranty. - REDACTED Content

5.5 Support Services and TAM Warranty - REDACTED Content

5.6 Warranty Remedies. Except for the Service Credits described in the Product Sheets, the remedies stated in Sections 5.2 through 5.5 above are the sole remedies, and Zscaler's sole obligation, with respect to Products that fail to comply with the warranties detailed in Sections 5.2 to 5.5.

5.7 Disclaimer of Warranties. - REDACTED Content

5.8 Scalability Warranty. - REDACTED Content

6. CONFIDENTIAL INFORMATION

6.1 Definition of Confidential Information. As used herein, "Confidential Information" means all confidential and proprietary information of a party ("**Disclosing Party**") disclosed to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information or the circumstances of disclosure, including the terms and conditions of this Agreement (including pricing and other terms reflected in all Orders hereunder), the Customer Data, the Products, the Zscaler Materials, Zscaler's security information and reports, and each party's respective business and marketing plans, technology and technical information, product designs, and business processes. The obligations in this Section shall not apply to any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party and without an obligation of confidentiality; (iii) was independently developed by the Receiving Party without the use of or reference to the Confidential Information of the Disclosing Party; or (iv) is lawfully received from a third party without breach of any obligation owed to the Disclosing Party and without an obligation of confidentiality.

6.2 Confidentiality. The Receiving Party shall not disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, except with the Disclosing Party's prior written permission. Either party may disclose Confidential Information to its personnel and its auditors who are subject to the same confidentiality obligations, and may disclose Confidential Information to its attorneys and accountants who are either subject to professional obligations of confidentiality or have agreed to be bound by confidentiality obligations at least as protective as those set out herein.

6.3 Protection. Receiving Party will use at least the same level of care to prevent unauthorized use of the Confidential Information as it uses for its own confidential and proprietary information of like kind, but in no event less than a reasonable standard of care.

6.4 Compelled Disclosure. If the Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of such compelled disclosure, to the extent legally permitted, and reasonable assistance, at Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

6.5 Remedies. If the Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the Disclosing Party in breach of the confidentiality protections hereunder, or if the Receiving Party is compelled to disclose (or is likely to become compelled to disclose) any Confidential Information of the Disclosing Party pursuant to Section 6.4, the Disclosing Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts or seek a protective order regarding such acts.

7. TERM AND TERMINATION

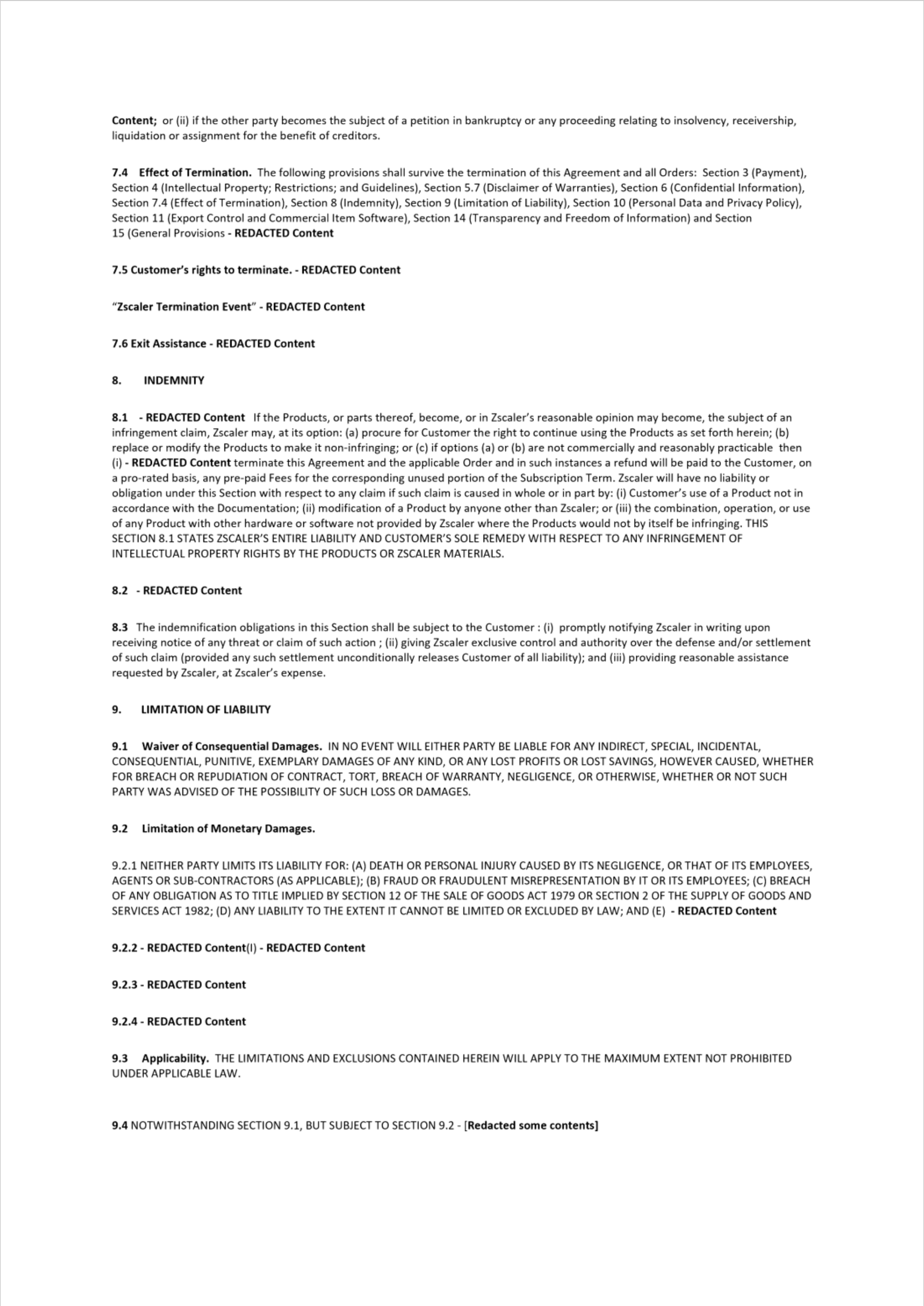
7.1 Agreement Term. This Agreement shall continue in effect for the Subscription Term unless terminated earlier in accordance with this Agreement.

7.2. Order Term. The term of Customer's subscription to the Products will begin on the start date set forth in an Order and will continue for the period of time stated in the Order ("**Initial Subscription Term**") unless terminated earlier in accordance with this Agreement. No less than six (6) months prior to the end of the Initial Subscription Term, the parties will work together to agree on the length and pricing for a renewal term ("**Renewal Subscription Term**"); otherwise, Customer's subscription will terminate at the end of the Initial Subscription Term (or the then-applicable Renewal Subscription Term. [**Redacted some contents]**

7.3 Termination for Material Breach. Either party may terminate this Agreement and any Order: (i) if the other party breaches any terms and conditions of this Agreement and does not cure such breach within thirty (30) days of receiving notice of such breach. - **REDACTED**

Page 6

30 June 2020 14:55



Content; or (ii) if the other party becomes the subject of a petition in bankruptcy or any proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

7.4 Effect of Termination. The following provisions shall survive the termination of this Agreement and all Orders: Section 3 (Payment), Section 4 (Intellectual Property; Restrictions; and Guidelines), Section 5.7 (Disclaimer of Warranties), Section 6 (Confidential Information), Section 7.4 (Effect of Termination), Section 8 (Indemnity), Section 9 (Limitation of Liability), Section 10 (Personal Data and Privacy Policy), Section 11 (Export Control and Commercial Item Software), Section 14 (Transparency and Freedom of Information) and Section 15 (General Provisions **- REDACTED Content**

7.5 Customer's rights to terminate. - REDACTED Content

"Zscaler Termination Event" - REDACTED Content

7.6 Exit Assistance - REDACTED Content

8. INDEMNITY

8.1 - REDACTED Content If the Products, or parts thereof, become, or in Zscaler's reasonable opinion may become, the subject of an infringement claim, Zscaler may, at its option: (a) procure for Customer the right to continue using the Products as set forth herein; (b) replace or modify the Products to make it non-infringing; or (c) if options (a) or (b) are not commercially and reasonably practicable then (i) **- REDACTED Content** terminate this Agreement and the applicable Order and in such instances a refund will be paid to the Customer, on a pro-rated basis, any pre-paid Fees for the corresponding unused portion of the Subscription Term. Zscaler will have no liability or obligation under this Section with respect to any claim if such claim is caused in whole or in part by: (i) Customer's use of a Product not in accordance with the Documentation; (ii) modification of a Product by anyone other than Zscaler; or (iii) the combination, operation, or use of any Product with other hardware or software not provided by Zscaler where the Products would not by itself be infringing. THIS SECTION 8.1 STATES ZSCALER'S ENTIRE LIABILITY AND CUSTOMER'S SOLE REMEDY WITH RESPECT TO ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS BY THE PRODUCTS OR ZSCALER MATERIALS.

8.2 - REDACTED Content

8.3 The indemnification obligations in this Section shall be subject to the Customer : (i) promptly notifying Zscaler in writing upon receiving notice of any threat or claim of such action ; (ii) giving Zscaler exclusive control and authority over the defense and/or settlement of such claim (provided any such settlement unconditionally releases Customer of all liability); and (iii) providing reasonable assistance requested by Zscaler, at Zscaler's expense.

9. LIMITATION OF LIABILITY

9.1 Waiver of Consequential Damages. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY DAMAGES OF ANY KIND, OR ANY LOST PROFITS OR LOST SAVINGS, HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT SUCH PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

9.2 Limitation of Monetary Damages.

9.2.1 NEITHER PARTY LIMITS ITS LIABILITY FOR: (A) DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE, OR THAT OF ITS EMPLOYEES, AGENTS OR SUB-CONTRACTORS (AS APPLICABLE); (B) FRAUD OR FRAUDULENT MISREPRESENTATION BY IT OR ITS EMPLOYEES; (C) BREACH OF ANY OBLIGATION AS TO TITLE IMPLIED BY SECTION 12 OF THE SALE OF GOODS ACT 1979 OR SECTION 2 OF THE SUPPLY OF GOODS AND SERVICES ACT 1982; (D) ANY LIABILITY TO THE EXTENT IT CANNOT BE LIMITED OR EXCLUDED BY LAW; AND (E) **- REDACTED Content**

9.2.2 - REDACTED Content(I) **- REDACTED Content**

9.2.3 - REDACTED Content

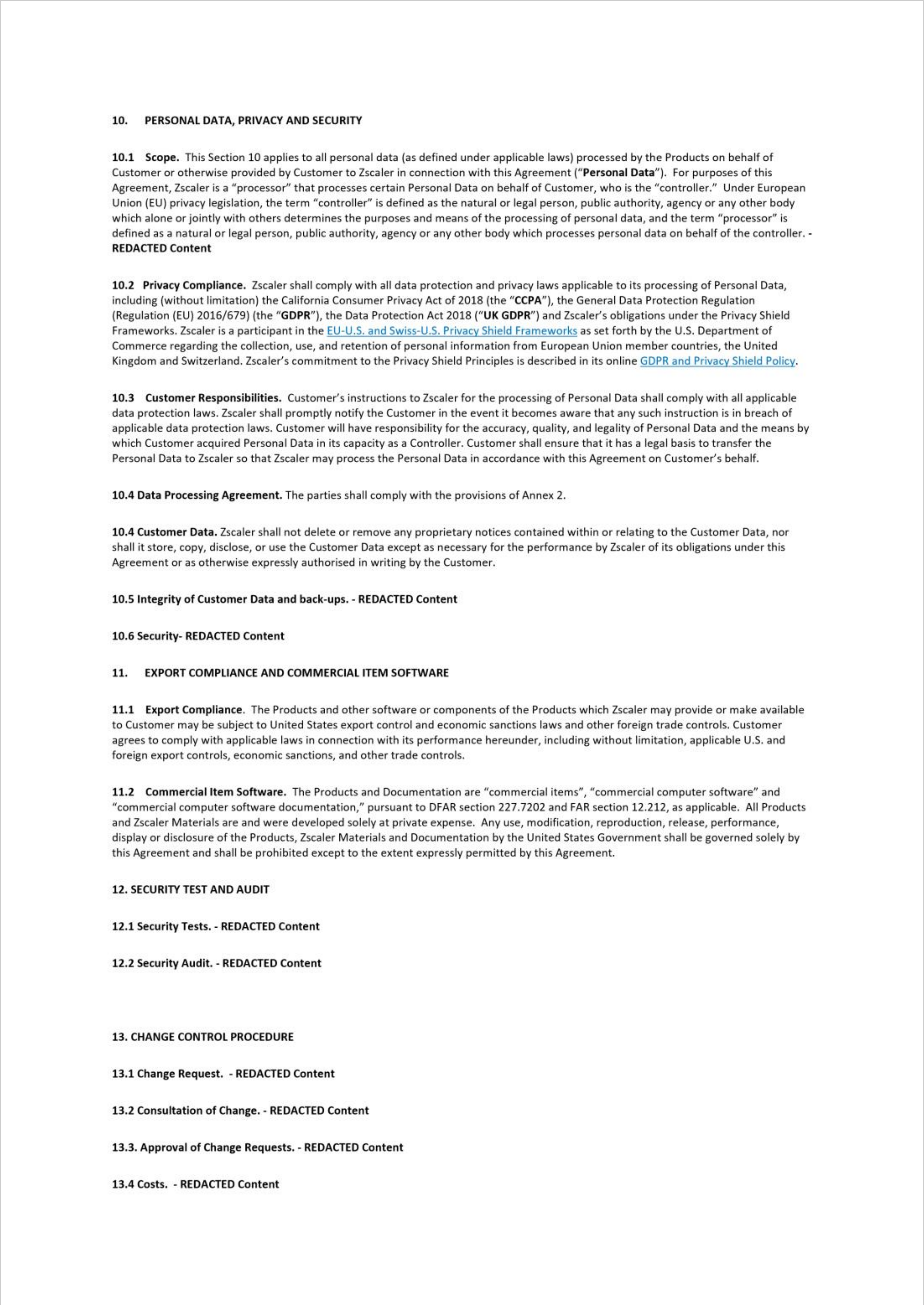
9.2.4 - REDACTED Content

9.3 Applicability. THE LIMITATIONS AND EXCLUSIONS CONTAINED HEREIN WILL APPLY TO THE MAXIMUM EXTENT NOT PROHIBITED UNDER APPLICABLE LAW.

9.4 NOTWITHSTANDING SECTION 9.1, BUT SUBJECT TO SECTION 9.2 - [**Redacted some contents]**

Page 7

30 June 2020 14:55



10. PERSONAL DATA, PRIVACY AND SECURITY

10.1 Scope. This Section 10 applies to all personal data (as defined under applicable laws) processed by the Products on behalf of Customer or otherwise provided by Customer to Zscaler in connection with this Agreement ("**Personal Data**"). For purposes of this Agreement, Zscaler is a "processor" that processes certain Personal Data on behalf of Customer, who is the "controller." Under European Union (EU) privacy legislation, the term "controller" is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, and the term "processor" is defined as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. - **REDACTED Content**

10.2 Privacy Compliance. Zscaler shall comply with all data protection and privacy laws applicable to its processing of Personal Data, including (without limitation) the California Consumer Privacy Act of 2018 (the "**CCPA**"), the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"), the Data Protection Act 2018 ("**UK GDPR**") and Zscaler's obligations under the Privacy Shield Frameworks. Zscaler is a participant in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries, the United Kingdom and Switzerland. Zscaler's commitment to the Privacy Shield Principles is described in its online GDPR and Privacy Shield Policy.

10.3 Customer Responsibilities. Customer's instructions to Zscaler for the processing of Personal Data shall comply with all applicable data protection laws. Zscaler shall promptly notify the Customer in the event it becomes aware that any such instruction is in breach of applicable data protection laws. Customer will have responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data in its capacity as a Controller. Customer shall ensure that it has a legal basis to transfer the Personal Data to Zscaler so that Zscaler may process the Personal Data in accordance with this Agreement on Customer's behalf.

10.4 Data Processing Agreement. The parties shall comply with the provisions of Annex 2.

10.4 Customer Data. Zscaler shall not delete or remove any proprietary notices contained within or relating to the Customer Data, nor shall it store, copy, disclose, or use the Customer Data except as necessary for the performance by Zscaler of its obligations under this Agreement or as otherwise expressly authorised in writing by the Customer.

10.5 Integrity of Customer Data and back-ups. - REDACTED Content

10.6 Security- REDACTED Content

11. EXPORT COMPLIANCE AND COMMERCIAL ITEM SOFTWARE

11.1 Export Compliance. The Products and other software or components of the Products which Zscaler may provide or make available to Customer may be subject to United States export control and economic sanctions laws and other foreign trade controls. Customer agrees to comply with applicable laws in connection with its performance hereunder, including without limitation, applicable U.S. and foreign export controls, economic sanctions, and other trade controls.

11.2 Commercial Item Software. The Products and Documentation are "commercial items", "commercial computer software" and "commercial computer software documentation," pursuant to DFAR section 227.7202 and FAR section 12.212, as applicable. All Products and Zscaler Materials are and were developed solely at private expense. Any use, modification, reproduction, release, performance, display or disclosure of the Products, Zscaler Materials and Documentation by the United States Government shall be governed solely by this Agreement and shall be prohibited except to the extent expressly permitted by this Agreement.

12. SECURITY TEST AND AUDIT

12.1 Security Tests. - REDACTED Content

12.2 Security Audit. - REDACTED Content

13. CHANGE CONTROL PROCEDURE

13.1 Change Request. - REDACTED Content

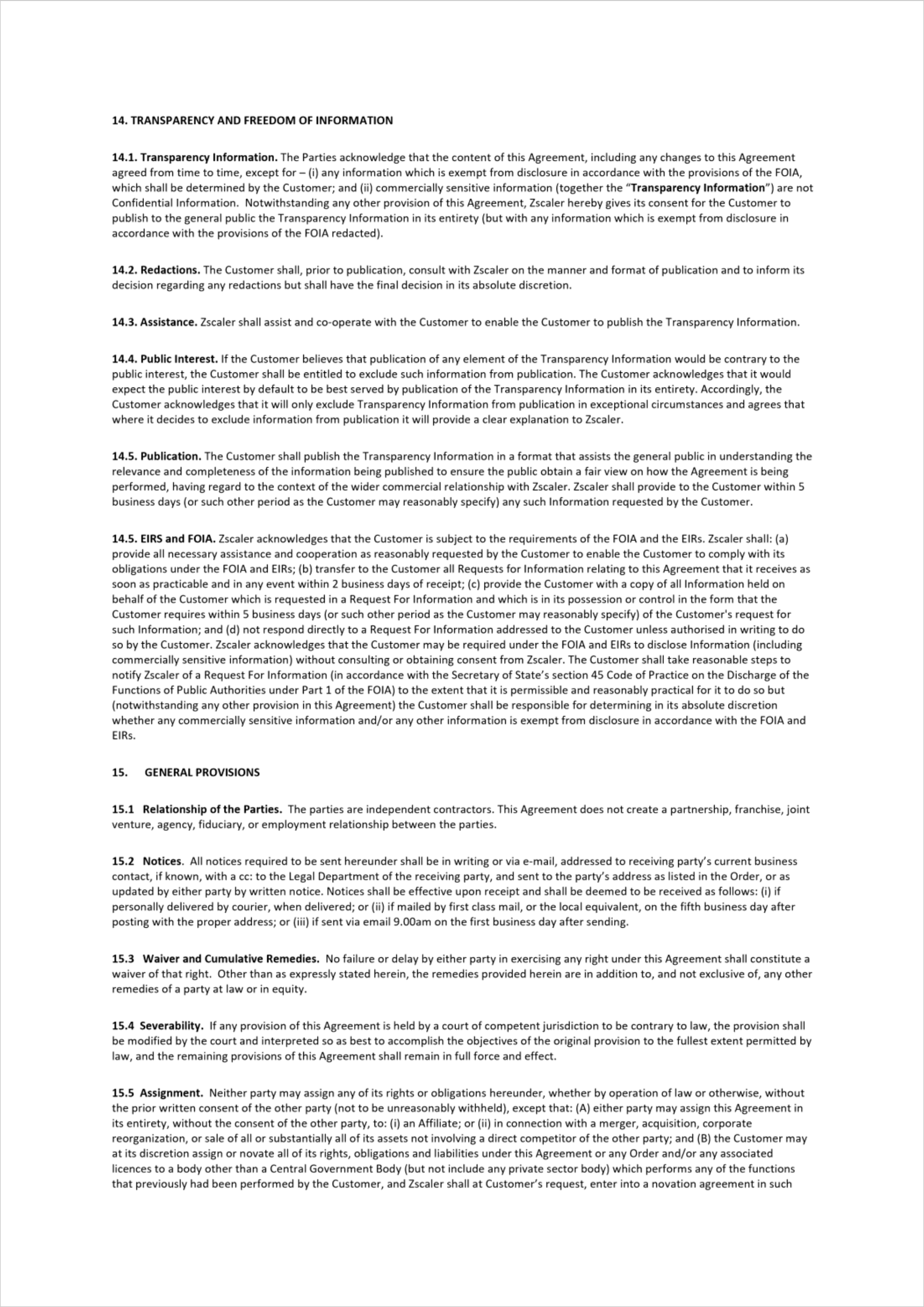
13.2 Consultation of Change. - REDACTED Content

13.3. Approval of Change Requests. - REDACTED Content

13.4 Costs. - REDACTED Content

Page 8

30 June 2020 14:55



14. TRANSPARENCY AND FREEDOM OF INFORMATION

14.1. Transparency Information. The Parties acknowledge that the content of this Agreement, including any changes to this Agreement agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Customer; and (ii) commercially sensitive information (together the "**Transparency Information**") are not Confidential Information. Notwithstanding any other provision of this Agreement, Zscaler hereby gives its consent for the Customer to publish to the general public the Transparency Information in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted).

14.2. Redactions. The Customer shall, prior to publication, consult with Zscaler on the manner and format of publication and to inform its decision regarding any redactions but shall have the final decision in its absolute discretion.

14.3. Assistance. Zscaler shall assist and co-operate with the Customer to enable the Customer to publish the Transparency Information.

14.4. Public Interest. If the Customer believes that publication of any element of the Transparency Information would be contrary to the public interest, the Customer shall be entitled to exclude such information from publication. The Customer acknowledges that it would expect the public interest by default to be best served by publication of the Transparency Information in its entirety. Accordingly, the Customer acknowledges that it will only exclude Transparency Information from publication in exceptional circumstances and agrees that where it decides to exclude information from publication it will provide a clear explanation to Zscaler.

14.5. Publication. The Customer shall publish the Transparency Information in a format that assists the general public in understanding the relevance and completeness of the information being published to ensure the public obtain a fair view on how the Agreement is being performed, having regard to the context of the wider commercial relationship with Zscaler. Zscaler shall provide to the Customer within 5 business days (or such other period as the Customer may reasonably specify) any such Information requested by the Customer.

14.5. EIRS and FOIA. Zscaler acknowledges that the Customer is subject to the requirements of the FOIA and the EIRs. Zscaler shall: (a) provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and EIRs; (b) transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 business days of receipt; (c) provide the Customer with a copy of all Information held on behalf of the Customer which is requested in a Request For Information and which is in its possession or control in the form that the Customer requires within 5 business days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and (d) not respond directly to a Request For Information addressed to the Customer unless authorised in writing to do so by the Customer. Zscaler acknowledges that the Customer may be required under the FOIA and EIRs to disclose Information (including commercially sensitive information) without consulting or obtaining consent from Zscaler. The Customer shall take reasonable steps to notify Zscaler of a Request For Information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Agreement) the Customer shall be responsible for determining in its absolute discretion whether any commercially sensitive information and/or any other information is exempt from disclosure in accordance with the FOIA and EIRs.

15. GENERAL PROVISIONS

15.1 Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties.

15.2 Notices. All notices required to be sent hereunder shall be in writing or via e-mail, addressed to receiving party's current business contact, if known, with a cc: to the Legal Department of the receiving party, and sent to the party's address as listed in the Order, or as updated by either party by written notice. Notices shall be effective upon receipt and shall be deemed to be received as follows: (i) if personally delivered by courier, when delivered; or (ii) if mailed by first class mail, or the local equivalent, on the fifth business day after posting with the proper address; or (iii) if sent via email 9.00am on the first business day after sending.

15.3 Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

15.4 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in full force and effect.

15.5 Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld), except that: (A) either party may assign this Agreement in its entirety, without the consent of the other party, to: (i) an Affiliate; or (ii) in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party; and (B) the Customer may at its discretion assign or novate all of its rights, obligations and liabilities under this Agreement or any Order and/or any associated licences to a body other than a Central Government Body (but not include any private sector body) which performs any of the functions that previously had been performed by the Customer, and Zscaler shall at Customer's request, enter into a novation agreement in such

Page 9

30 June 2020 14:55

form as the parties shall agree to enable Customer to exercise its rights pursuant to this Section 15.5. Any attempt by a party to assign its rights or obligations under this Agreement in breach of this Section shall be void and of no effect. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

A change in the legal status of the Customer such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and the Orders and this Agreement and its Orders shall be binding on any successor body to the Customer.

15.6 Dispute Resolution- REDACTED Content

15.7 Governing Law and Jurisdiction. This Agreement and any issues, disputes or claims arising out of or related hereto shall be governed by and construed in accordance with the laws of England and Wales, without giving effect to its conflicts of laws rules, the United Nations Convention on the International Sale of Goods, or the Uniform Computer Information Transactions Act. Subject to Section 15.6 above (including the Customer's right to refer the dispute to arbitration), the parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

15.8 Force Majeure. Neither party shall be liable for delay or non-performance of its obligations hereunder (or part thereof) if the cause of delay or non-performance is due to a Force Majeure Event. The party affected shall be relieved from its obligations (or part thereof) for the time that the Force Majeure Event lasts and hinders the performance of said obligations (or part thereof). The party affected shall promptly notify the other party and make reasonable efforts to mitigate the effects of the Force Majeure Event.

15.9 Entire Agreement. This Agreement, including the Product Sheets, constitutes the entire agreement between the parties, and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. The parties are not relying and have not relied on any representations or warranties whatsoever regarding the subject matter of this Agreement, express or implied, except for the representations and warranties set forth in this Agreement. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. No terms or conditions set forth on any purchase order, preprinted form or other document shall add to or vary the terms and conditions of this Agreement, and all such terms or conditions shall be null and void.

15.10. Insurance. Zscaler shall at its own cost be solely responsible for taking out and maintaining in force during the Subscription Term insurance and for a period of not less than six (6) years after expiry of the Order entered into hereunder, with one or more reputable insurers, such policy or policies of insurance it may reasonably consider adequate, and in accordance with Good Industry Practice to cover its potential liabilities with, and arising out of, this Agreement or any Orders.

15.11 Third Party Rights. A person who is not a Party to this Agreement or the relevant Order has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement or the relevant Order but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that act.

15.12 Prevention of Fraud and Bribery

15.12.1- REDACTED Content

15.12.2- REDACTED Content

15.12.3- REDACTED Content

15.12.4. - REDACTED Content

15.12.5. - REDACTED Content

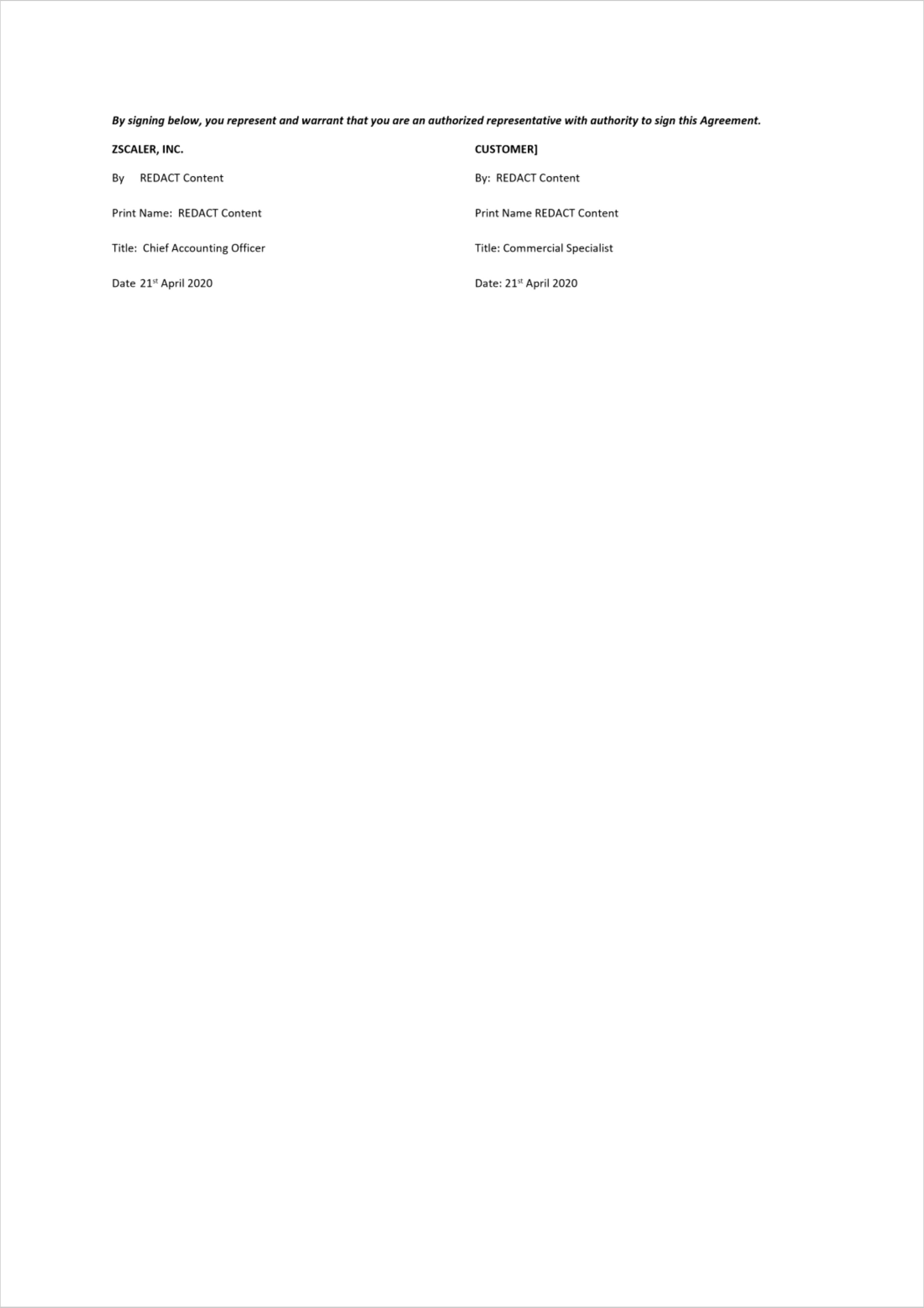
15.12.6. - REDACTED Content

15.13 Publicity and branding. Zscaler shall not: (a) make any press announcements or publicise this Agreement or any Order or its contents in any way; or (b) use the Customer's name or brand in any promotion or marketing or announcement of orders, without approval of the Customer. Notwithstanding the foregoing, Zscaler shall be permitted to include Customer's name in any sales related materials confirming Zscaler's current customer base, provided that such materials shall not be distributed other than to existing and potential future Zscaler customers.

15.14 Variation. No variation to this Agreement (including this Section 15.14) shall be effective unless made in accordance with Section 13 (Change Control Procedure) (or otherwise agreed in writing) and signed by a duly authorised officer of each of the Customer and Zscaler.

Page 10

30 June 2020 14:55



By signing below, you represent and warrant that you are an authorized representative with authority to sign this Agreement.

ZSCALER, INC.

By REDACT Content

Print Name: REDACT Content

Title: Chief Accounting Officer

Date 21st April 2020

CUSTOMER]

By: REDACT Content

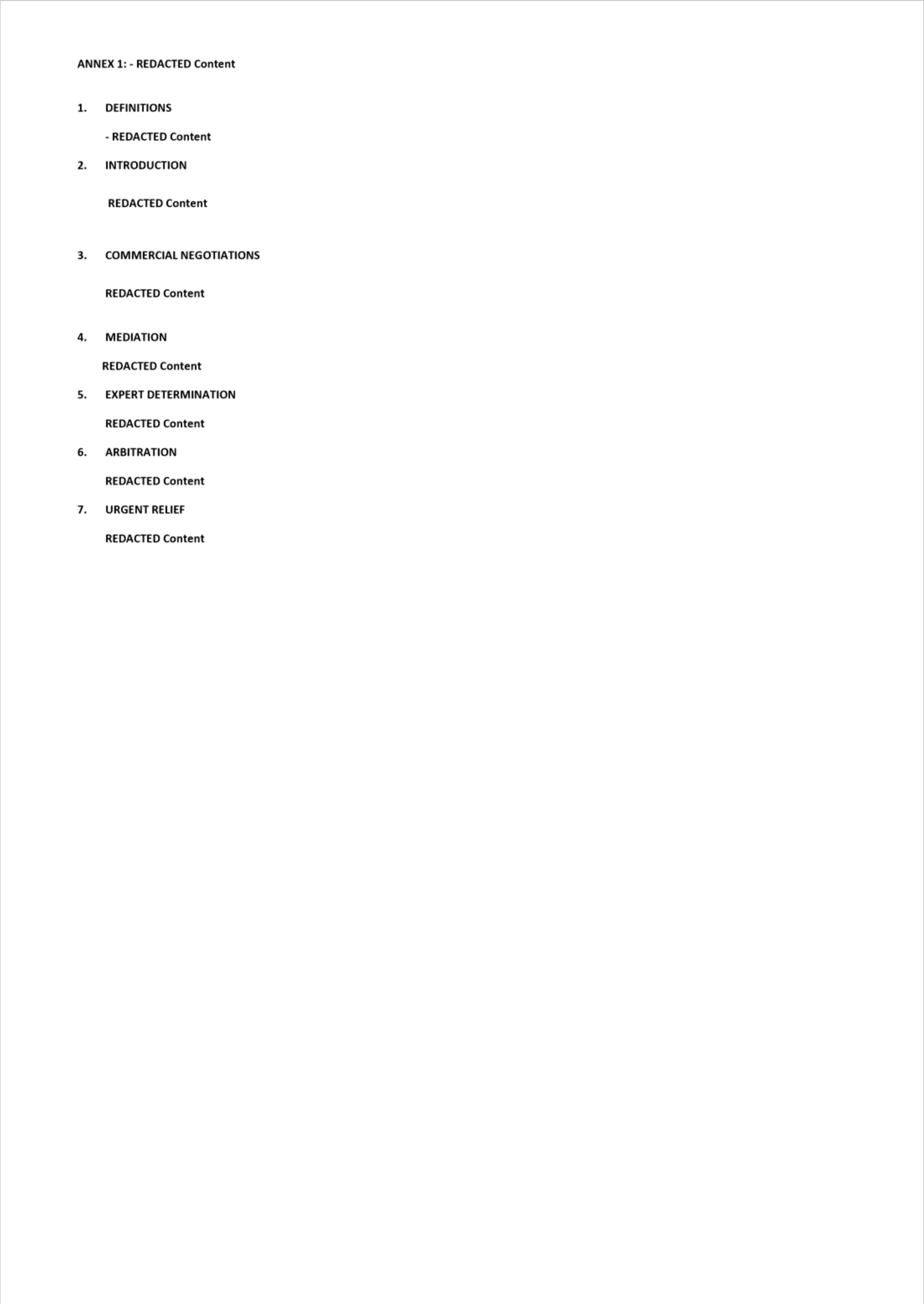
Print Name REDACT Content

Title: Commercial Specialist

Date: 21st April 2020

Page 11

30 June 2020 14:55



ANNEX 1: - REDACTED Content

1. **DEFINITIONS**

   - REDACTED Content

2. **INTRODUCTION**

   REDACTED Content

3. **COMMERCIAL NEGOTIATIONS**

   REDACTED Content

4. **MEDIATION**

   REDACTED Content

5. **EXPERT DETERMINATION**

   REDACTED Content

6. **ARBITRATION**

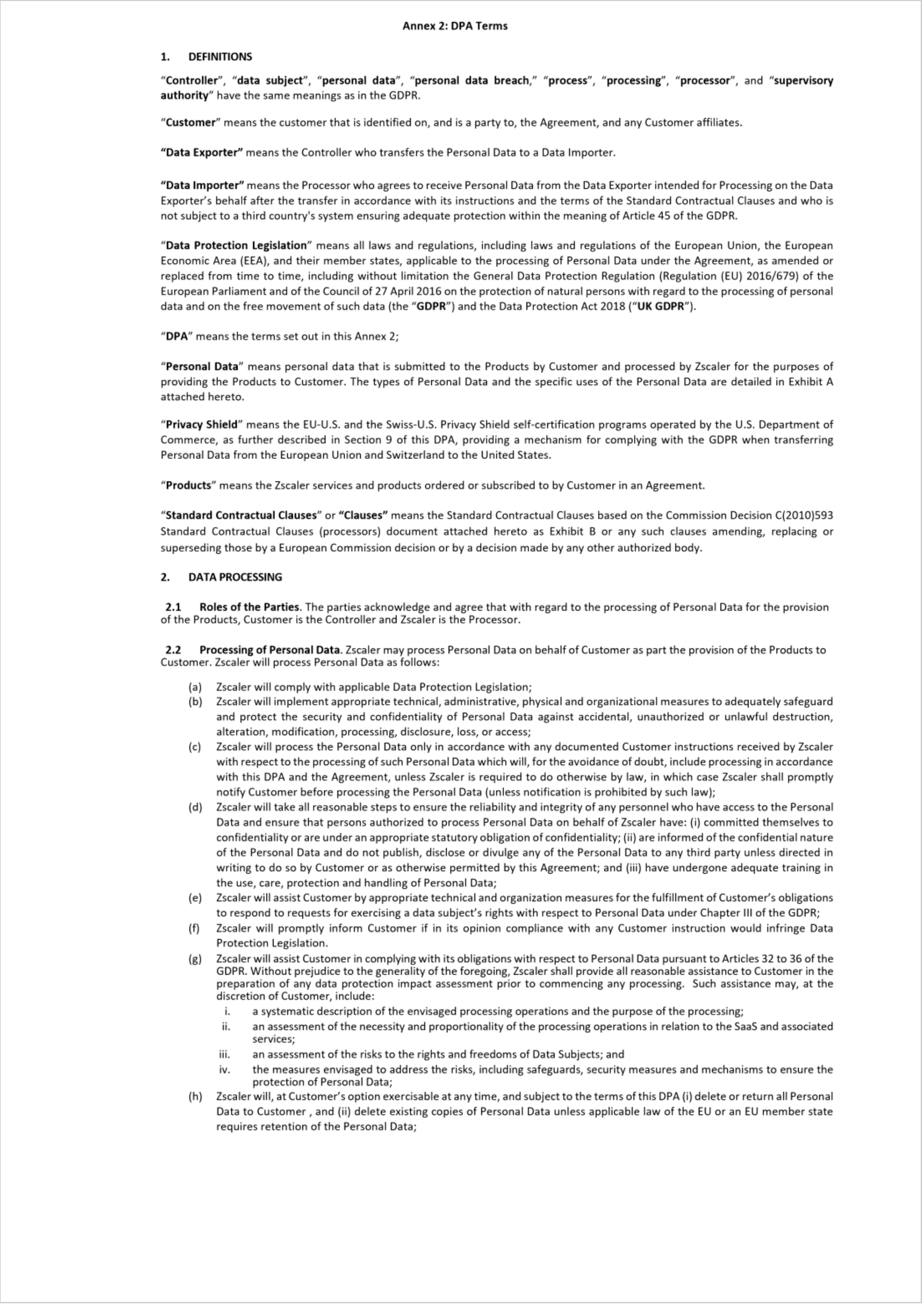
   REDACTED Content

7. **URGENT RELIEF**

   REDACTED Content

Page 12

30 June 2020 14:55



Annex 2: DPA Terms

1. DEFINITIONS

"**Controller**", "**data subject**", "**personal data**", "**personal data breach**," "**process**", "**processing**", "**processor**", and "**supervisory authority**" have the same meanings as in the GDPR.

"**Customer**" means the customer that is identified on, and is a party to, the Agreement, and any Customer affiliates.

"Data Exporter" means the Controller who transfers the Personal Data to a Data Importer.

"Data Importer" means the Processor who agrees to receive Personal Data from the Data Exporter intended for Processing on the Data Exporter's behalf after the transfer in accordance with its instructions and the terms of the Standard Contractual Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 45 of the GDPR.

"**Data Protection Legislation**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area (EEA), and their member states, applicable to the processing of Personal Data under the Agreement, as amended or replaced from time to time, including without limitation the General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**") and the Data Protection Act 2018 ("**UK GDPR**").

"**DPA**" means the terms set out in this Annex 2;

"**Personal Data**" means personal data that is submitted to the Products by Customer and processed by Zscaler for the purposes of providing the Products to Customer. The types of Personal Data and the specific uses of the Personal Data are detailed in Exhibit A attached hereto.

"**Privacy Shield**" means the EU-U.S. and the Swiss-U.S. Privacy Shield self-certification programs operated by the U.S. Department of Commerce, as further described in Section 9 of this DPA, providing a mechanism for complying with the GDPR when transferring Personal Data from the European Union and Switzerland to the United States.

"**Products**" means the Zscaler services and products ordered or subscribed to by Customer in an Agreement.

"**Standard Contractual Clauses**" or **"Clauses"** means the Standard Contractual Clauses based on the Commission Decision C(2010)593 Standard Contractual Clauses (processors) document attached hereto as Exhibit B or any such clauses amending, replacing or superseding those by a European Commission decision or by a decision made by any other authorized body.

2. DATA PROCESSING

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Personal Data for the provision of the Products, Customer is the Controller and Zscaler is the Processor.

2.2 Processing of Personal Data. Zscaler may process Personal Data on behalf of Customer as part the provision of the Products to Customer. Zscaler will process Personal Data as follows:

(a) Zscaler will comply with applicable Data Protection Legislation;

(b) Zscaler will implement appropriate technical, administrative, physical and organizational measures to adequately safeguard and protect the security and confidentiality of Personal Data against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access;

(c) Zscaler will process the Personal Data only in accordance with any documented Customer instructions received by Zscaler with respect to the processing of such Personal Data which will, for the avoidance of doubt, include processing in accordance with this DPA and the Agreement, unless Zscaler is required to do otherwise by law, in which case Zscaler shall promptly notify Customer before processing the Personal Data (unless notification is prohibited by such law);

(d) Zscaler will take all reasonable steps to ensure the reliability and integrity of any personnel who have access to the Personal Data and ensure that persons authorized to process Personal Data on behalf of Zscaler have: (i) committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (ii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by Customer or as otherwise permitted by this Agreement; and (iii) have undergone adequate training in the use, care, protection and handling of Personal Data;

(e) Zscaler will assist Customer by appropriate technical and organization measures for the fulfillment of Customer's obligations to respond to requests for exercising a data subject's rights with respect to Personal Data under Chapter III of the GDPR;

(f) Zscaler will promptly inform Customer if in its opinion compliance with any Customer instruction would infringe Data Protection Legislation.

(g) Zscaler will assist Customer in complying with its obligations with respect to Personal Data pursuant to Articles 32 to 36 of the GDPR. Without prejudice to the generality of the foregoing, Zscaler shall provide all reasonable assistance to Customer in the preparation of any data protection impact assessment prior to commencing any processing. Such assistance may, at the discretion of Customer, include:

   i. a systematic description of the envisaged processing operations and the purpose of the processing;

   ii. an assessment of the necessity and proportionality of the processing operations in relation to the SaaS and associated services;

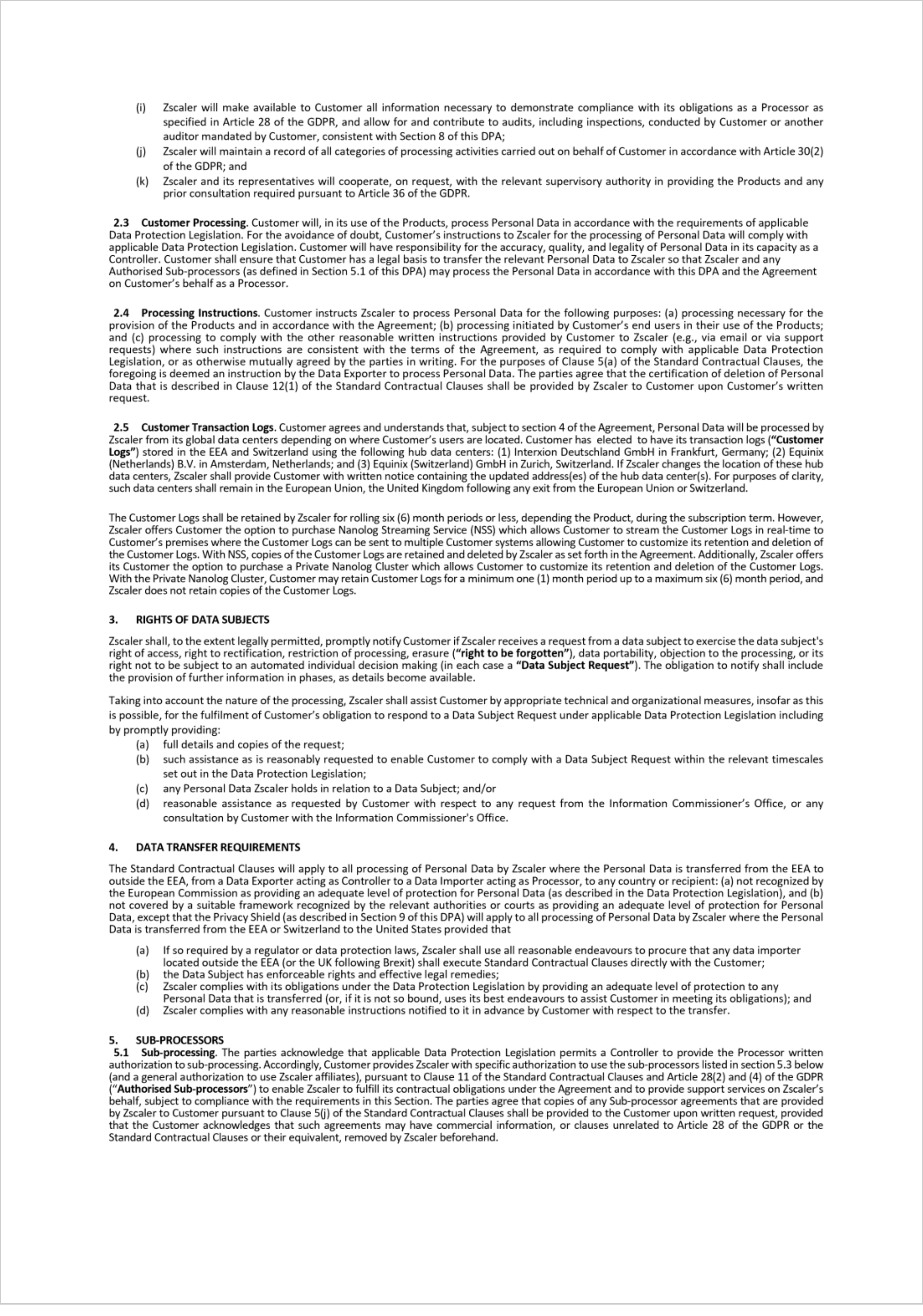
   iii. an assessment of the risks to the rights and freedoms of Data Subjects; and

   iv. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data;

(h) Zscaler will, at Customer's option exercisable at any time, and subject to the terms of this DPA (i) delete or return all Personal Data to Customer , and (ii) delete existing copies of Personal Data unless applicable law of the EU or an EU member state requires retention of the Personal Data;

Page 13

30 June 2020 14:55



(i) Zscaler will make available to Customer all information necessary to demonstrate compliance with its obligations as a Processor as specified in Article 28 of the GDPR, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, consistent with Section 8 of this DPA;

(j) Zscaler will maintain a record of all categories of processing activities carried out on behalf of Customer in accordance with Article 30(2) of the GDPR; and

(k) Zscaler and its representatives will cooperate, on request, with the relevant supervisory authority in providing the Products and any prior consultation required pursuant to Article 36 of the GDPR.

2.3 Customer Processing. Customer will, in its use of the Products, process Personal Data in accordance with the requirements of applicable Data Protection Legislation. For the avoidance of doubt, Customer's instructions to Zscaler for the processing of Personal Data will comply with applicable Data Protection Legislation. Customer will have responsibility for the accuracy, quality, and legality of Personal Data in its capacity as a Controller. Customer shall ensure that Customer has a legal basis to transfer the relevant Personal Data to Zscaler so that Zscaler and any Authorised Sub-processors (as defined in Section 5.1 of this DPA) may process the Personal Data in accordance with this DPA and the Agreement on Customer's behalf as a Processor.

2.4 Processing Instructions. Customer instructs Zscaler to process Personal Data for the following purposes: (a) processing necessary for the provision of the Products and in accordance with the Agreement; (b) processing initiated by Customer's end users in their use of the Products; and (c) processing to comply with the other reasonable written instructions provided by Customer to Zscaler (e.g., via email or via support requests) where such instructions are consistent with the terms of the Agreement, as required to comply with applicable Data Protection Legislation, or as otherwise mutually agreed by the parties in writing. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the foregoing is deemed an instruction by the Data Exporter to process Personal Data. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Zscaler to Customer upon Customer's written request.

2.5 Customer Transaction Logs. Customer agrees and understands that, subject to section 4 of the Agreement, Personal Data will be processed by Zscaler from its global data centers depending on where Customer's users are located. Customer has elected to have its transaction logs (**"Customer Logs"**) stored in the EEA and Switzerland using the following hub data centers: (1) Interxion Deutschland GmbH in Frankfurt, Germany; (2) Equinix (Netherlands) B.V. in Amsterdam, Netherlands; and (3) Equinix (Switzerland) GmbH in Zurich, Switzerland. If Zscaler changes the location of these hub data centers, Zscaler shall provide Customer with written notice containing the updated address(es) of the hub data center(s). For purposes of clarity, such data centers shall remain in the European Union, the United Kingdom following any exit from the European Union or Switzerland.

The Customer Logs shall be retained by Zscaler for rolling six (6) month periods or less, depending the Product, during the subscription term. However, Zscaler offers Customer the option to purchase Nanolog Streaming Service (NSS) which allows Customer to stream the Customer Logs in real-time to Customer's premises where the Customer Logs can be sent to multiple Customer systems allowing Customer to customize its retention and deletion of the Customer Logs. With NSS, copies of the Customer Logs are retained and deleted by Zscaler as set forth in the Agreement. Additionally, Zscaler offers its Customer the option to purchase a Private Nanolog Cluster which allows Customer to customize its retention and deletion of the Customer Logs. With the Private Nanolog Cluster, Customer may retain Customer Logs for a minimum one (1) month period up to a maximum six (6) month period, and Zscaler does not retain copies of the Customer Logs.

3. RIGHTS OF DATA SUBJECTS

Zscaler shall, to the extent legally permitted, promptly notify Customer if Zscaler receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure (**"right to be forgotten"**), data portability, objection to the processing, or its right not to be subject to an automated individual decision making (in each case a **"Data Subject Request"**). The obligation to notify shall include the provision of further information in phases, as details become available.

Taking into account the nature of the processing, Zscaler shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Legislation including by promptly providing:

(a) full details and copies of the request;

(b) such assistance as is reasonably requested to enable Customer to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) any Personal Data Zscaler holds in relation to a Data Subject; and/or

(d) reasonable assistance as requested by Customer with respect to any request from the Information Commissioner's Office, or any consultation by Customer with the Information Commissioner's Office.

4. DATA TRANSFER REQUIREMENTS

The Standard Contractual Clauses will apply to all processing of Personal Data by Zscaler where the Personal Data is transferred from the EEA to outside the EEA, from a Data Exporter acting as Controller to a Data Importer acting as Processor, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Legislation), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, except that the Privacy Shield (as described in Section 9 of this DPA) will apply to all processing of Personal Data by Zscaler where the Personal Data is transferred from the EEA or Switzerland to the United States provided that

(a) If so required by a regulator or data protection laws, Zscaler shall use all reasonable endeavours to procure that any data importer located outside the EEA (or the UK following Brexit) shall execute Standard Contractual Clauses directly with the Customer;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) Zscaler complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist Customer in meeting its obligations); and

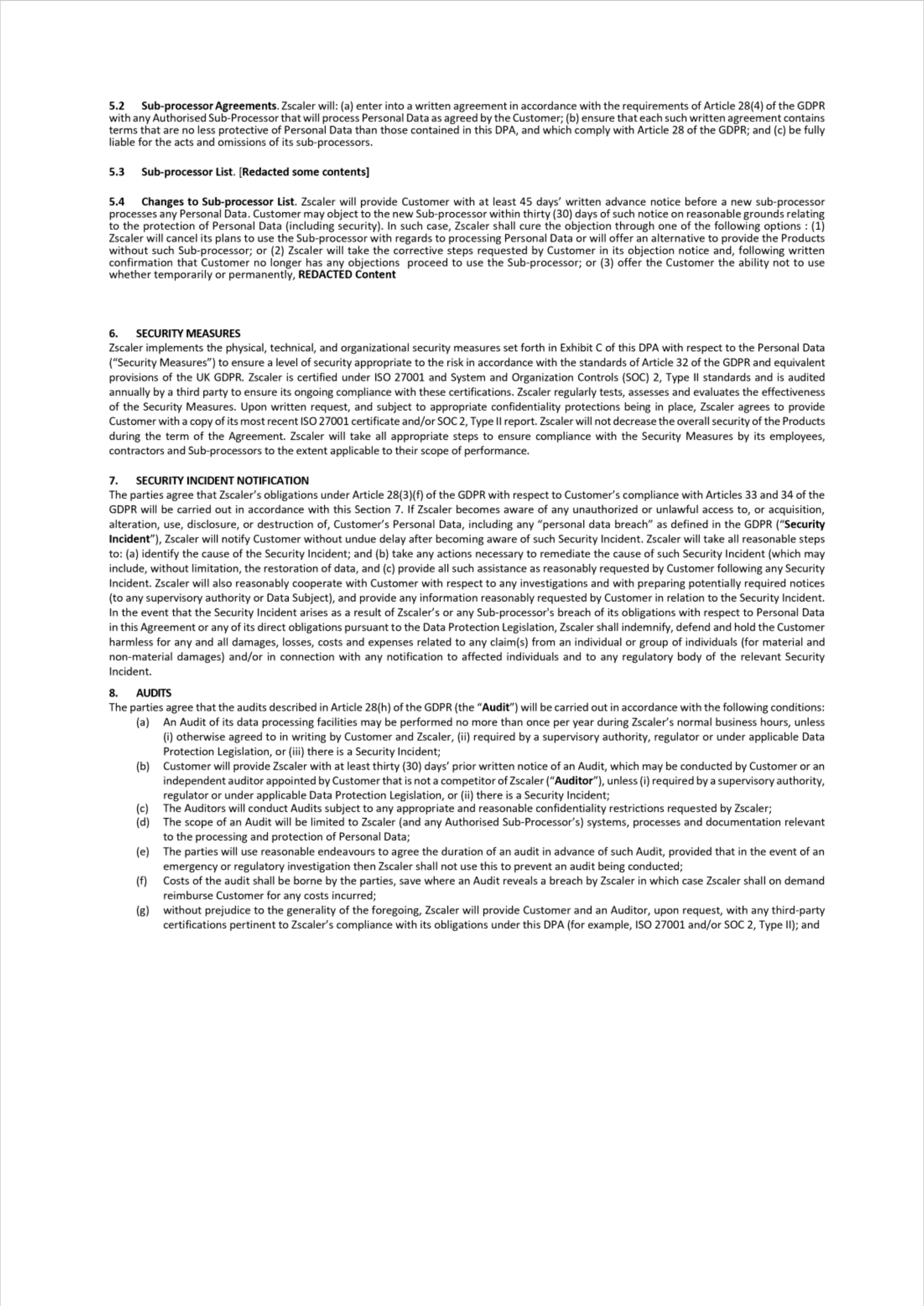
(d) Zscaler complies with any reasonable instructions notified to it in advance by Customer with respect to the transfer.

5. SUB-PROCESSORS

5.1 Sub-processing. The parties acknowledge that applicable Data Protection Legislation permits a Controller to provide the Processor written authorization to sub-processing. Accordingly, Customer provides Zscaler with specific authorization to use the sub-processors listed in section 5.3 below (and a general authorization to use Zscaler affiliates), pursuant to Clause 11 of the Standard Contractual Clauses and Article 28(2) and (4) of the GDPR ("**Authorised Sub-processors**") to enable Zscaler to fulfill its contractual obligations under the Agreement and to provide support services on Zscaler's behalf, subject to compliance with the requirements in this Section. The parties agree that copies of any Sub-processor agreements that are provided by Zscaler to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses shall be provided to the Customer upon written request, provided that the Customer acknowledges that such agreements may have commercial information, or clauses unrelated to Article 28 of the GDPR or the Standard Contractual Clauses or their equivalent, removed by Zscaler beforehand.

Page 14

30 June 2020 14:55



5.2 Sub-processor Agreements. Zscaler will: (a) enter into a written agreement in accordance with the requirements of Article 28(4) of the GDPR with any Authorised Sub-Processor that will process Personal Data as agreed by the Customer; (b) ensure that each such written agreement contains terms that are no less protective of Personal Data than those contained in this DPA, and which comply with Article 28 of the GDPR; and (c) be fully liable for the acts and omissions of its sub-processors.

5.3 Sub-processor List. [**Redacted some contents]**

5.4 Changes to Sub-processor List. Zscaler will provide Customer with at least 45 days' written advance notice before a new sub-processor processes any Personal Data. Customer may object to the new Sub-processor within thirty (30) days of such notice on reasonable grounds relating to the protection of Personal Data (including security). In such case, Zscaler shall cure the objection through one of the following options : (1) Zscaler will cancel its plans to use the Sub-processor with regards to processing Personal Data or will offer an alternative to provide the Products without such Sub-processor; or (2) Zscaler will take the corrective steps requested by Customer in its objection notice and, following written confirmation that Customer no longer has any objections proceed to use the Sub-processor; or (3) offer the Customer the ability not to use whether temporarily or permanently, **REDACTED Content**

6. SECURITY MEASURES

Zscaler implements the physical, technical, and organizational security measures set forth in Exhibit C of this DPA with respect to the Personal Data ("Security Measures") to ensure a level of security appropriate to the risk in accordance with the standards of Article 32 of the GDPR and equivalent provisions of the UK GDPR. Zscaler is certified under ISO 27001 and System and Organization Controls (SOC) 2, Type II standards and is audited annually by a third party to ensure its ongoing compliance with these certifications. Zscaler regularly tests, assesses and evaluates the effectiveness of the Security Measures. Upon written request, and subject to appropriate confidentiality protections being in place, Zscaler agrees to provide Customer with a copy of its most recent ISO 27001 certificate and/or SOC 2, Type II report. Zscaler will not decrease the overall security of the Products during the term of the Agreement. Zscaler will take all appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance.

7. SECURITY INCIDENT NOTIFICATION

The parties agree that Zscaler's obligations under Article 28(3)(f) of the GDPR with respect to Customer's compliance with Articles 33 and 34 of the GDPR will be carried out in accordance with this Section 7. If Zscaler becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer's Personal Data, including any "personal data breach" as defined in the GDPR ("**Security Incident**"), Zscaler will notify Customer without undue delay after becoming aware of such Security Incident. Zscaler will take all reasonable steps to: (a) identify the cause of the Security Incident; and (b) take any actions necessary to remediate the cause of such Security Incident (which may include, without limitation, the restoration of data, and (c) provide all such assistance as reasonably requested by Customer following any Security Incident. Zscaler will also reasonably cooperate with Customer with respect to any investigations and with preparing potentially required notices (to any supervisory authority or Data Subject), and provide any information reasonably requested by Customer in relation to the Security Incident. In the event that the Security Incident arises as a result of Zscaler's or any Sub-processor's breach of its obligations with respect to Personal Data in this Agreement or any of its direct obligations pursuant to the Data Protection Legislation, Zscaler shall indemnify, defend and hold the Customer harmless for any and all damages, losses, costs and expenses related to any claim(s) from an individual or group of individuals (for material and non-material damages) and/or in connection with any notification to affected individuals and to any regulatory body of the relevant Security Incident.

8. AUDITS

The parties agree that the audits described in Article 28(h) of the GDPR (the "**Audit**") will be carried out in accordance with the following conditions:

(a) An Audit of its data processing facilities may be performed no more than once per year during Zscaler's normal business hours, unless (i) otherwise agreed to in writing by Customer and Zscaler, (ii) required by a supervisory authority, regulator or under applicable Data Protection Legislation, or (iii) there is a Security Incident;

(b) Customer will provide Zscaler with at least thirty (30) days' prior written notice of an Audit, which may be conducted by Customer or an independent auditor appointed by Customer that is not a competitor of Zscaler ("**Auditor**"), unless (i) required by a supervisory authority, regulator or under applicable Data Protection Legislation, or (ii) there is a Security Incident;

(c) The Auditors will conduct Audits subject to any appropriate and reasonable confidentiality restrictions requested by Zscaler;

(d) The scope of an Audit will be limited to Zscaler (and any Authorised Sub-Processor's) systems, processes and documentation relevant to the processing and protection of Personal Data;

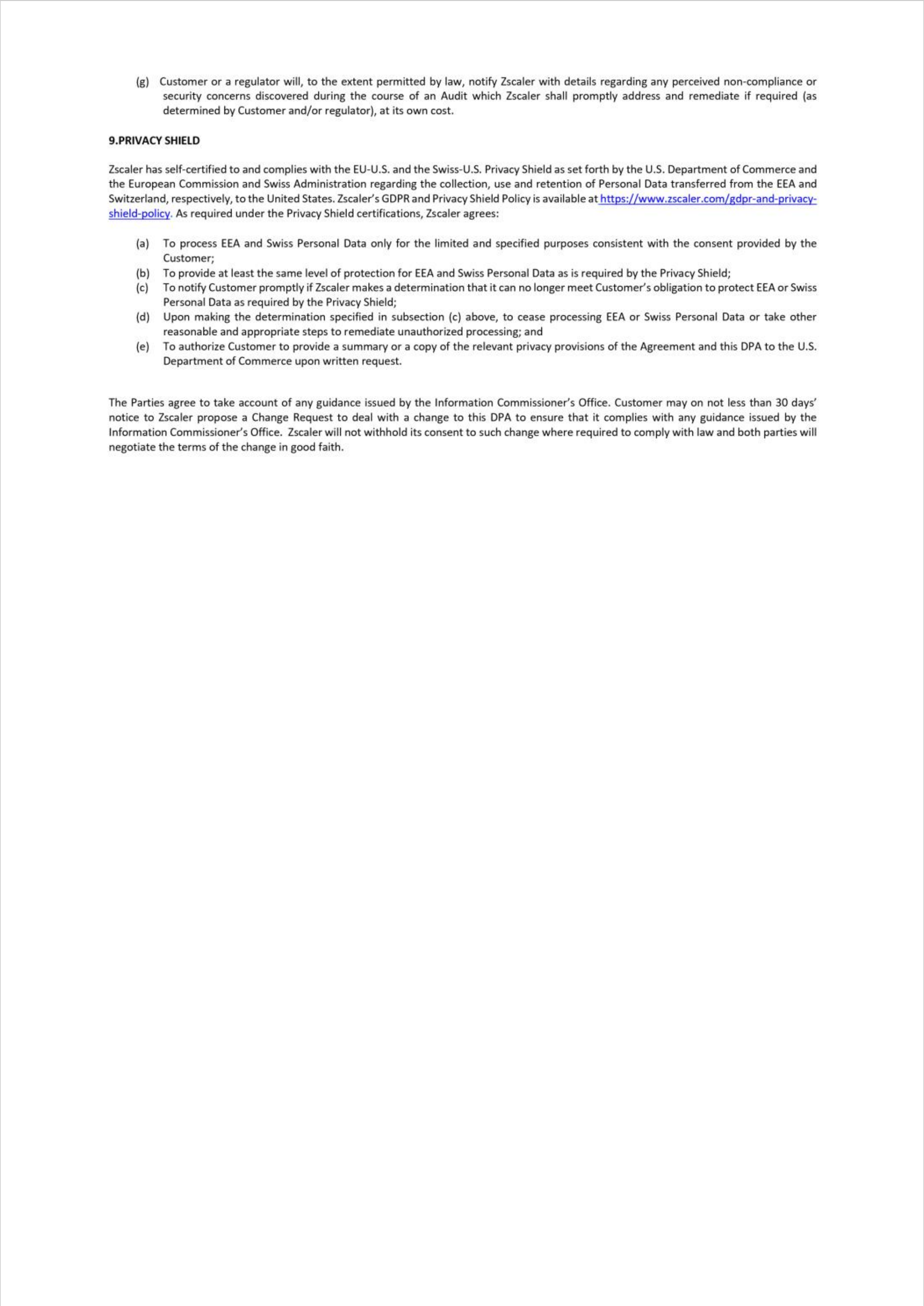
(e) The parties will use reasonable endeavours to agree the duration of an audit in advance of such Audit, provided that in the event of an emergency or regulatory investigation then Zscaler shall not use this to prevent an audit being conducted;

(f) Costs of the audit shall be borne by the parties, save where an Audit reveals a breach by Zscaler in which case Zscaler shall on demand reimburse Customer for any costs incurred;

(g) without prejudice to the generality of the foregoing, Zscaler will provide Customer and an Auditor, upon request, with any third-party certifications pertinent to Zscaler's compliance with its obligations under this DPA (for example, ISO 27001 and/or SOC 2, Type II); and

Page 15

30 June 2020 14:55



(g) Customer or a regulator will, to the extent permitted by law, notify Zscaler with details regarding any perceived non-compliance or security concerns discovered during the course of an Audit which Zscaler shall promptly address and remediate if required (as determined by Customer and/or regulator), at its own cost.

9.PRIVACY SHIELD

Zscaler has self-certified to and complies with the EU-U.S. and the Swiss-U.S. Privacy Shield as set forth by the U.S. Department of Commerce and the European Commission and Swiss Administration regarding the collection, use and retention of Personal Data transferred from the EEA and Switzerland, respectively, to the United States. Zscaler's GDPR and Privacy Shield Policy is available at https://www.zscaler.com/gdpr-and-privacy-shield-policy. As required under the Privacy Shield certifications, Zscaler agrees:

(a) To process EEA and Swiss Personal Data only for the limited and specified purposes consistent with the consent provided by the Customer;

(b) To provide at least the same level of protection for EEA and Swiss Personal Data as is required by the Privacy Shield;

(c) To notify Customer promptly if Zscaler makes a determination that it can no longer meet Customer's obligation to protect EEA or Swiss Personal Data as required by the Privacy Shield;

(d) Upon making the determination specified in subsection (c) above, to cease processing EEA or Swiss Personal Data or take other reasonable and appropriate steps to remediate unauthorized processing; and

(e) To authorize Customer to provide a summary or a copy of the relevant privacy provisions of the Agreement and this DPA to the U.S. Department of Commerce upon written request.

The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Customer may on not less than 30 days' notice to Zscaler propose a Change Request to deal with a change to this DPA to ensure that it complies with any guidance issued by the Information Commissioner's Office. Zscaler will not withhold its consent to such change where required to comply with law and both parties will negotiate the terms of the change in good faith.

Page 16

30 June 2020 14:55

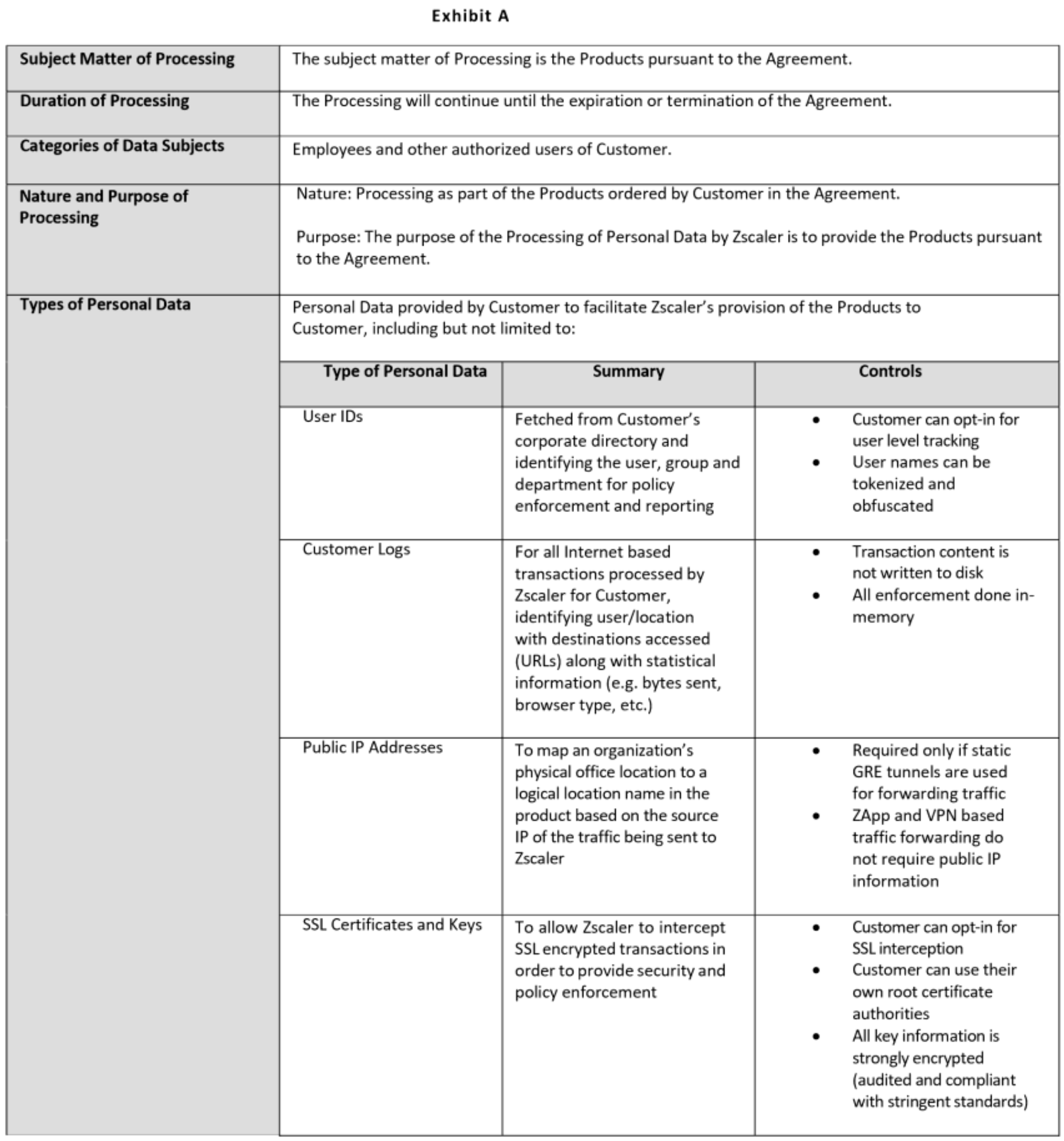


Exhibit A

Subject Matter of Processing	The subject matter of Processing is the Products pursuant to the Agreement.
Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
Categories of Data Subjects	Employees and other authorized users of Customer.
Nature and Purpose of Processing	Nature: Processing as part of the Products ordered by Customer in the Agreement. Purpose: The purpose of the Processing of Personal Data by Zscaler is to provide the Products pursuant to the Agreement.
Types of Personal Data	Personal Data provided by Customer to facilitate Zscaler's provision of the Products to Customer, including but not limited to:

Type of Personal Data	**Summary**	**Controls**
User IDs	Fetched from Customer's corporate directory and identifying the user, group and department for policy enforcement and reporting	• Customer can opt-in for user level tracking • User names can be tokenized and obfuscated
Customer Logs	For all Internet based transactions processed by Zscaler for Customer, identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.)	• Transaction content is not written to disk • All enforcement done in-memory
Public IP Addresses	To map an organization's physical office location to a logical location name in the product based on the source IP of the traffic being sent to Zscaler	• Required only if static GRE tunnels are used for forwarding traffic • ZApp and VPN based traffic forwarding do not require public IP information
SSL Certificates and Keys	To allow Zscaler to intercept SSL encrypted transactions in order to provide security and policy enforcement	• Customer can opt-in for SSL interception • Customer can use their own root certificate authorities • All key information is strongly encrypted (audited and compliant with stringent standards)

Page 17

30 June 2020 14:55

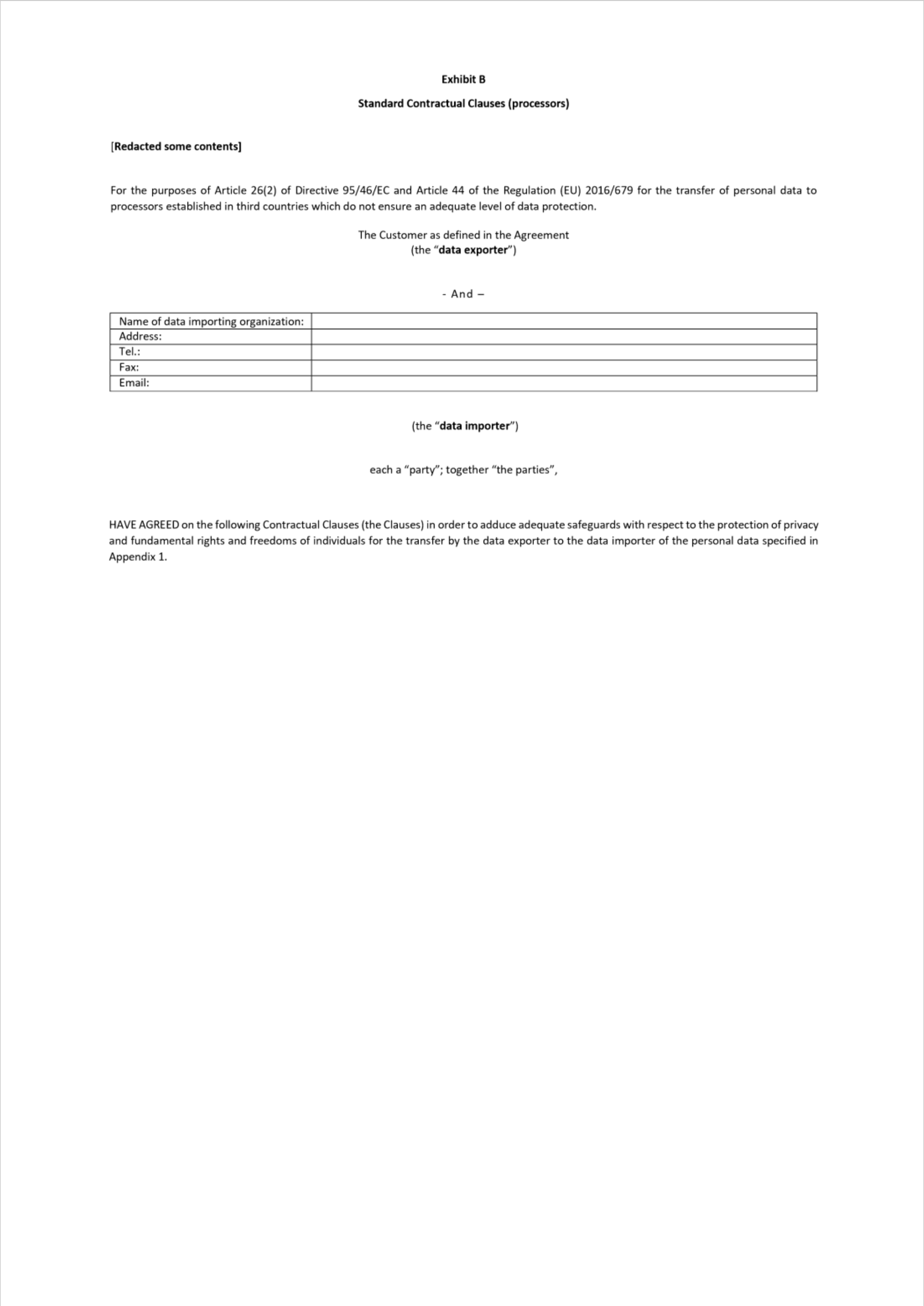


Exhibit B

Standard Contractual Clauses (processors)

[**Redacted some contents]**

For the purposes of Article 26(2) of Directive 95/46/EC and Article 44 of the Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The Customer as defined in the Agreement
(the “**data exporter**”)

- And –

Name of data importing organization:	
Address:	
Tel.:	
Fax:	
Email:	

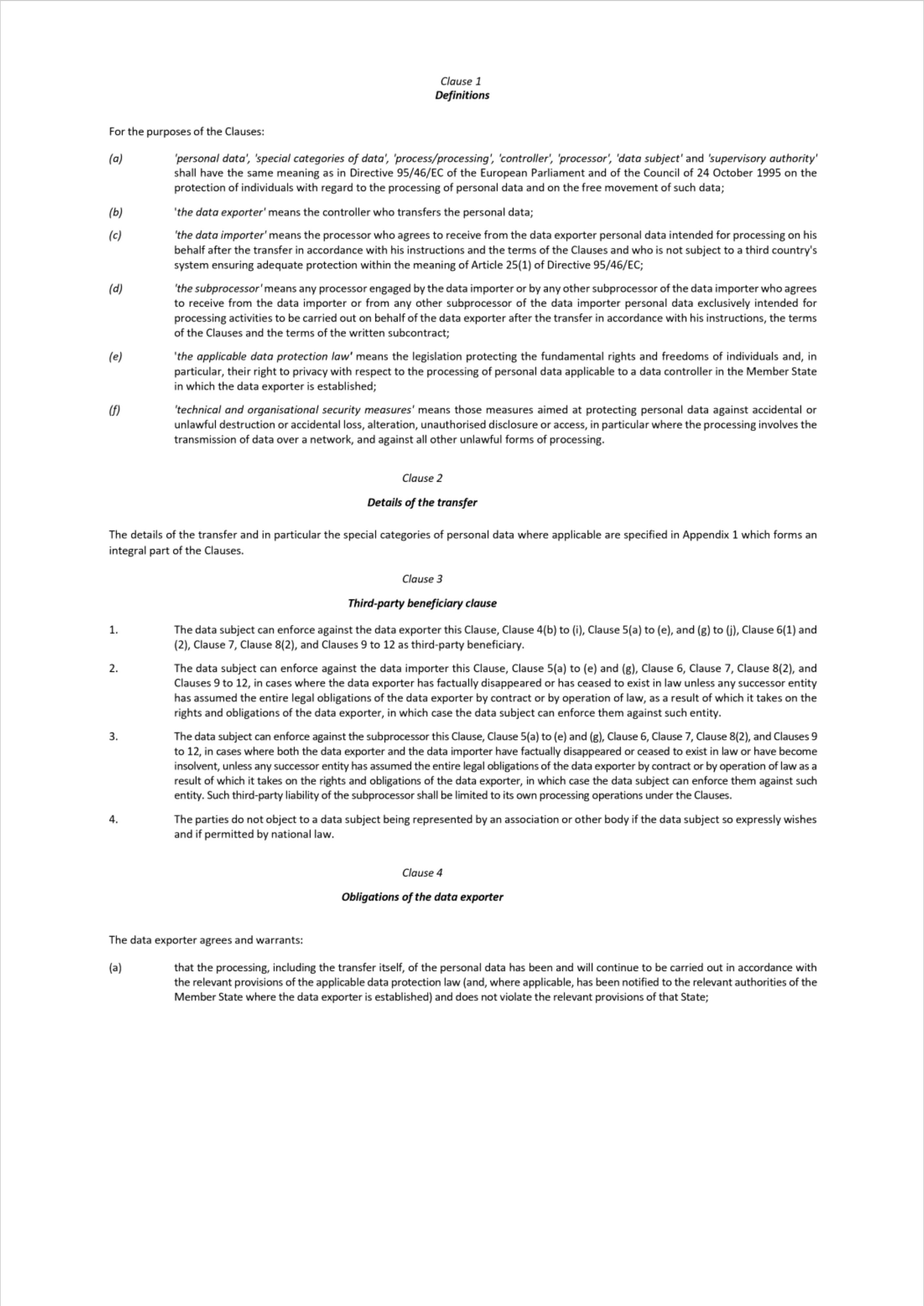
(the “**data importer**”)

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.

Page 18

30 June 2020 14:55



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;

(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.

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;

Page 19

30 June 2020 14:55

(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

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;

(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

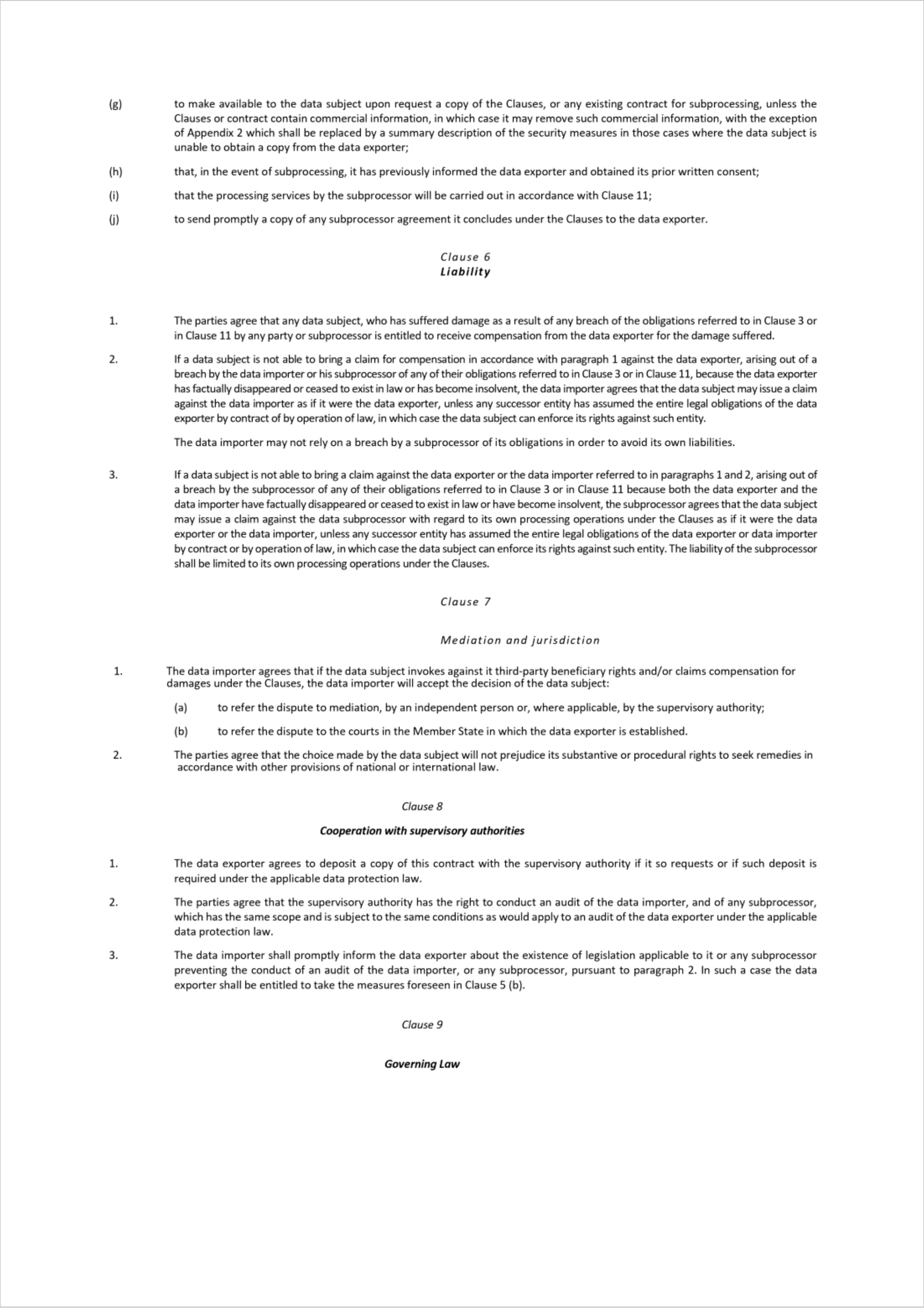
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(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;

Page 20

30 June 2020 14:55



(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.

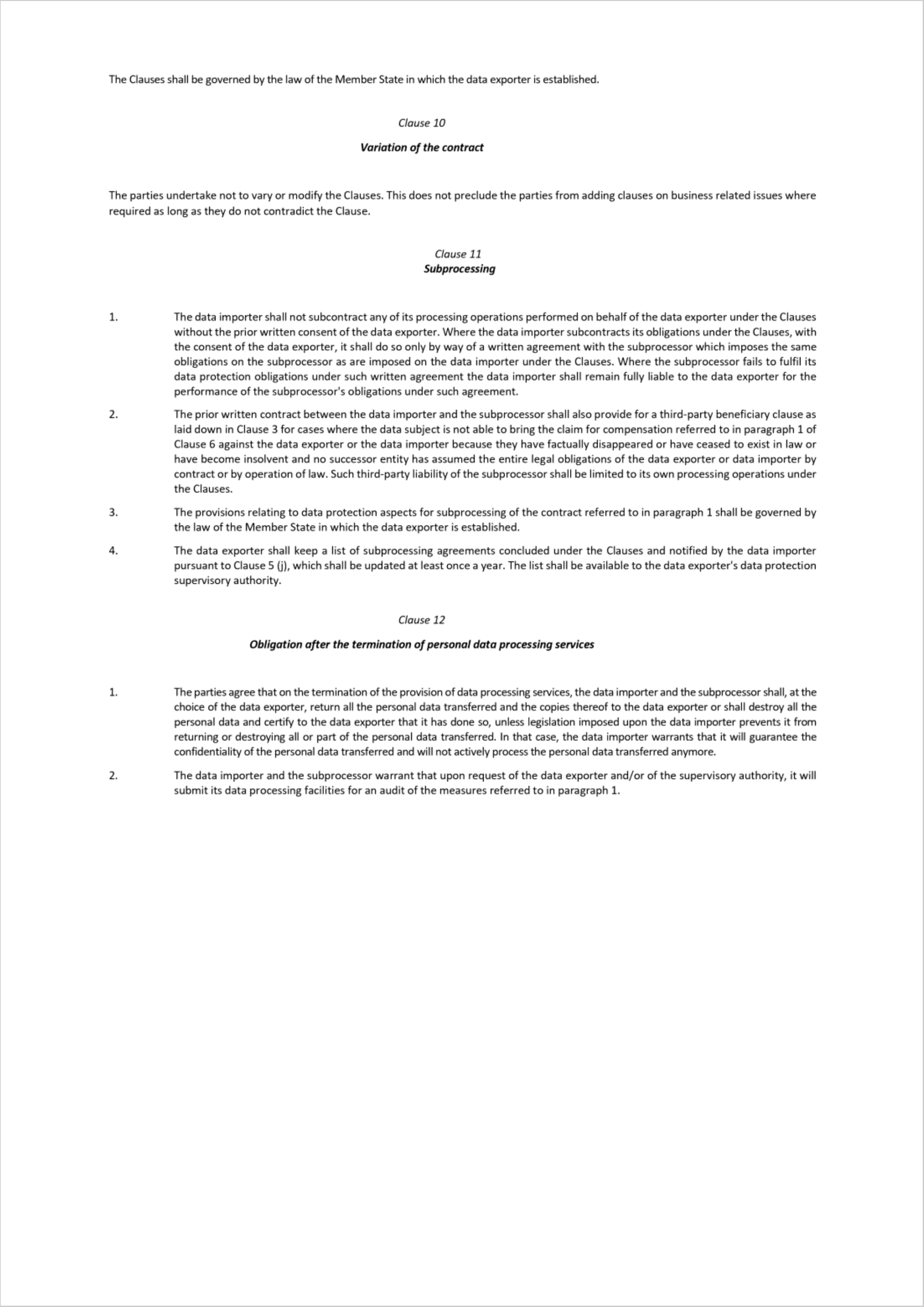
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures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

Clause 9

Governing Law

Page 21

30 June 2020 14:55



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. 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.

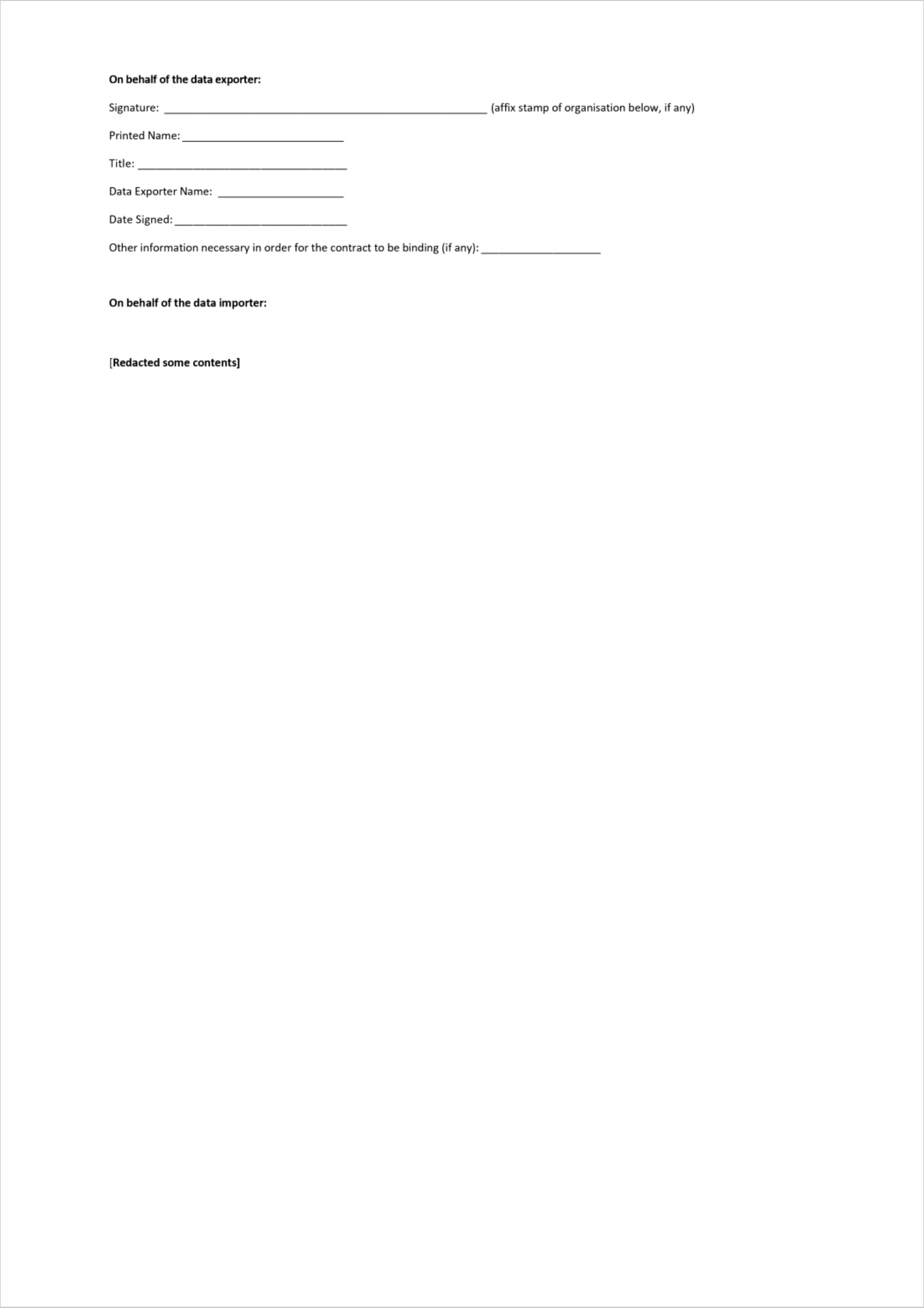
Clause 12

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.

Page 22

30 June 2020 14:55



On behalf of the data exporter:

Signature: ____ (affix stamp of organisation below, if any)

Printed Name: ________________________

Title: _______________________________

Data Exporter Name: ___________________

Date Signed: _________________________

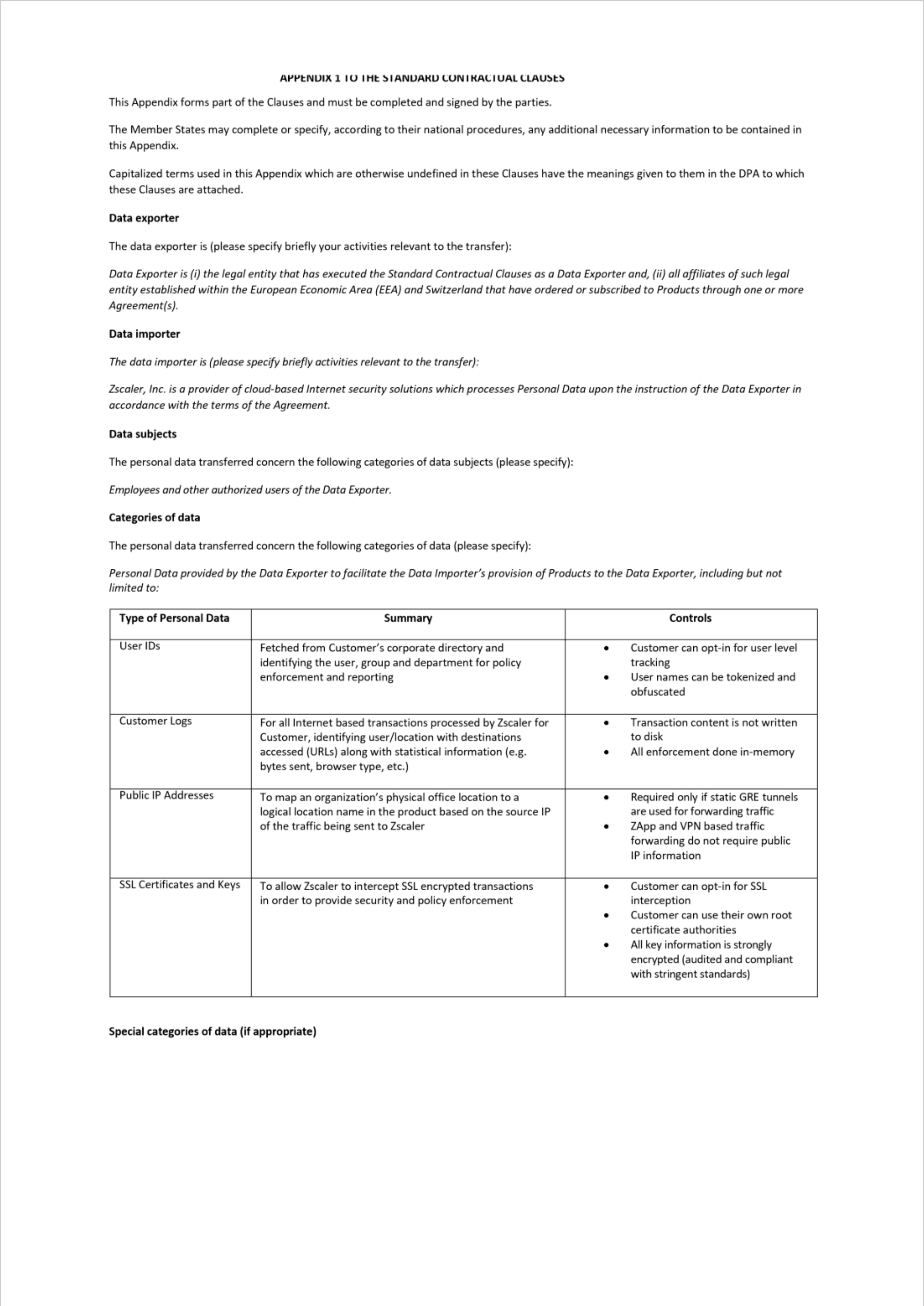
Other information necessary in order for the contract to be binding (if any): __________________

On behalf of the data importer:

[**Redacted some contents]**

Page 23

30 June 2020 14:55



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.

Capitalized terms used in this Appendix which are otherwise undefined in these Clauses have the meanings given to them in the DPA to which these Clauses are attached.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all affiliates of such legal entity established within the European Economic Area (EEA) and Switzerland that have ordered or subscribed to Products through one or more Agreement(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Zscaler, Inc. is a provider of cloud-based Internet security solutions which processes Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees and other authorized users of the Data Exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

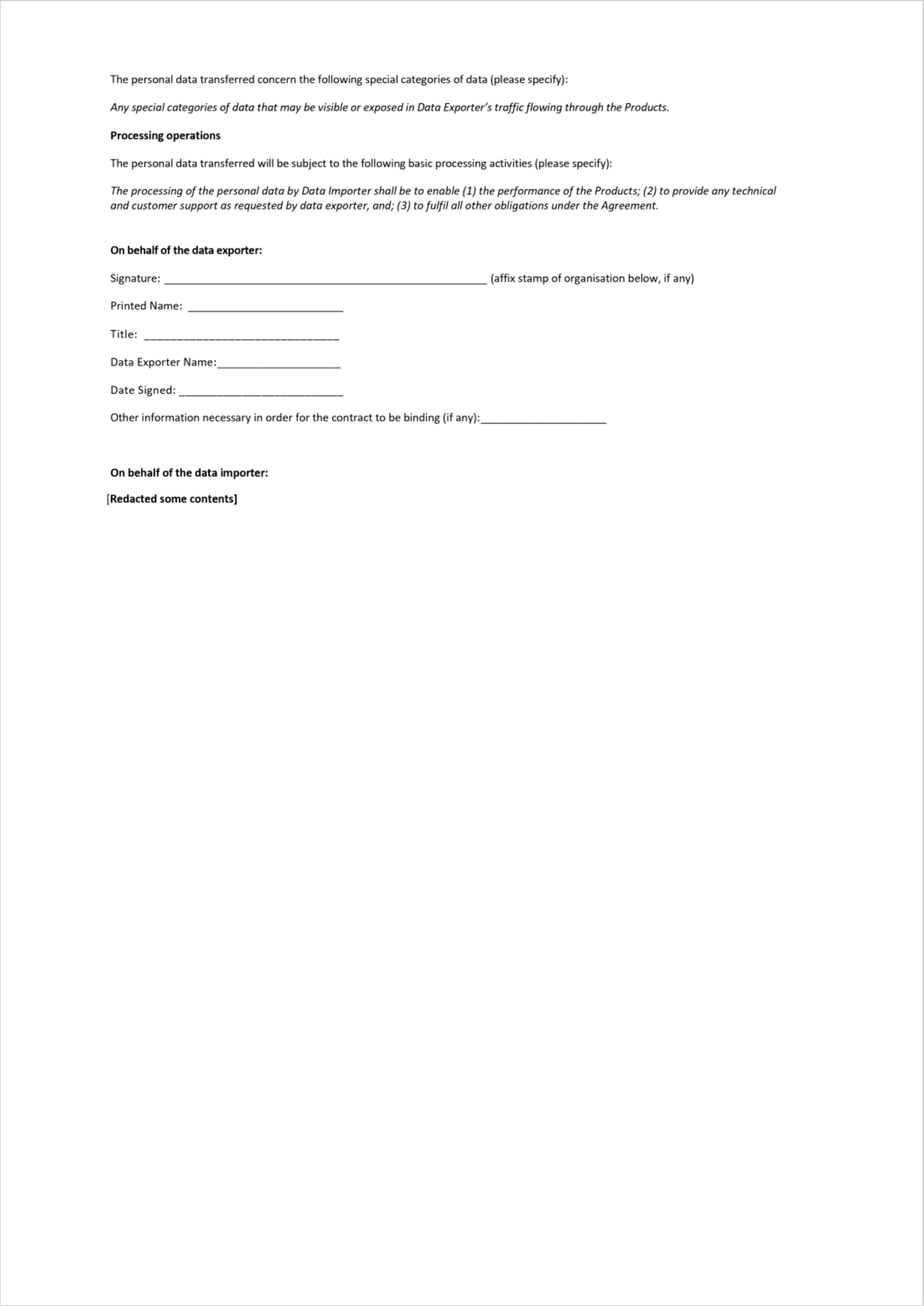
Personal Data provided by the Data Exporter to facilitate the Data Importer's provision of Products to the Data Exporter, including but not limited to:

Type of Personal Data	Summary	Controls
User IDs	Fetched from Customer's corporate directory and identifying the user, group and department for policy enforcement and reporting	• Customer can opt-in for user level tracking • User names can be tokenized and obfuscated
Customer Logs	For all Internet based transactions processed by Zscaler for Customer, identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.)	• Transaction content is not written to disk • All enforcement done in-memory
Public IP Addresses	To map an organization's physical office location to a logical location name in the product based on the source IP of the traffic being sent to Zscaler	• Required only if static GRE tunnels are used for forwarding traffic • ZApp and VPN based traffic forwarding do not require public IP information
SSL Certificates and Keys	To allow Zscaler to intercept SSL encrypted transactions in order to provide security and policy enforcement	• Customer can opt-in for SSL interception • Customer can use their own root certificate authorities • All key information is strongly encrypted (audited and compliant with stringent standards)

Special categories of data (if appropriate)

Page 24

30 June 2020 14:55



The personal data transferred concern the following special categories of data (please specify):

Any special categories of data that may be visible or exposed in Data Exporter's traffic flowing through the Products.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing of the personal data by Data Importer shall be to enable (1) the performance of the Products; (2) to provide any technical and customer support as requested by data exporter, and; (3) to fulfil all other obligations under the Agreement.

On behalf of the data exporter:

Signature: ____ (affix stamp of organisation below, if any)

Printed Name: ______________________

Title: ____________________________

Data Exporter Name:__________________

Date Signed: ________________________

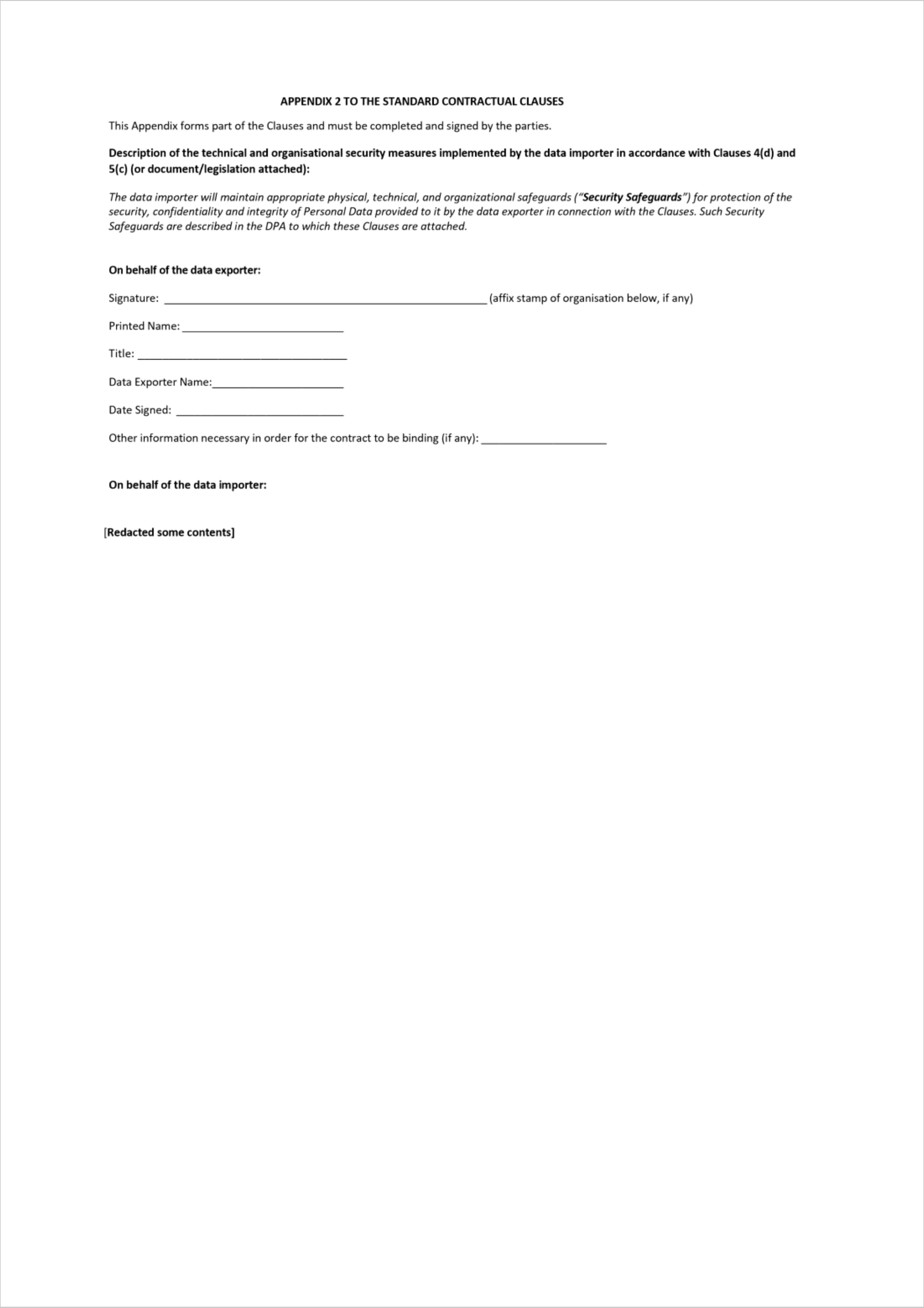
Other information necessary in order for the contract to be binding (if any):__________________

On behalf of the data importer:

[**Redacted some contents]**

Page 25

30 June 2020 14:55



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):

*The data importer will maintain appropriate physical, technical, and organizational safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of Personal Data provided to it by the data exporter in connection with the Clauses. Such Security Safeguards are described in the DPA to which these Clauses are attached.*

On behalf of the data exporter:

Signature: ____ (affix stamp of organisation below, if any)

Printed Name: ________________________

Title: _______________________________

Data Exporter Name:____________________

Date Signed: _________________________

Other information necessary in order for the contract to be binding (if any): ___________________

On behalf of the data importer:

[**Redacted some contents]**

Page 26

30 June 2020 14:55

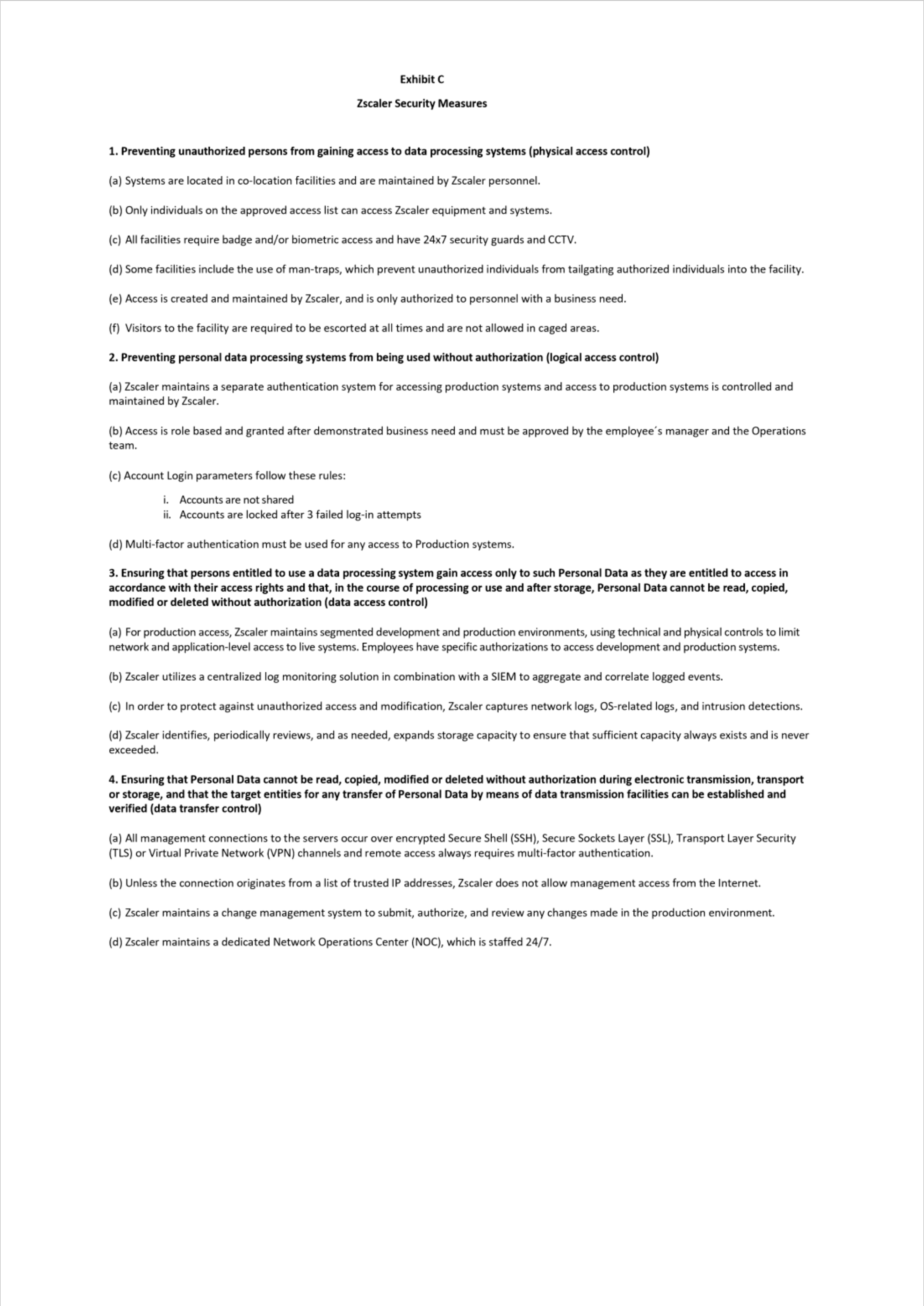


Exhibit C

Zscaler Security Measures

1. Preventing unauthorized persons from gaining access to data processing systems (physical access control)

(a) Systems are located in co-location facilities and are maintained by Zscaler personnel.

(b) Only individuals on the approved access list can access Zscaler equipment and systems.

(c) All facilities require badge and/or biometric access and have 24x7 security guards and CCTV.

(d) Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

(e) Access is created and maintained by Zscaler, and is only authorized to personnel with a business need.

(f) Visitors to the facility are required to be escorted at all times and are not allowed in caged areas.

2. Preventing personal data processing systems from being used without authorization (logical access control)

(a) Zscaler maintains a separate authentication system for accessing production systems and access to production systems is controlled and maintained by Zscaler.

(b) Access is role based and granted after demonstrated business need and must be approved by the employee´s manager and the Operations team.

(c) Account Login parameters follow these rules:

i. Accounts are not shared
ii. Accounts are locked after 3 failed log-in attempts

(d) Multi-factor authentication must be used for any access to Production systems.

3. Ensuring that persons entitled to use a data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control)

(a) For production access, Zscaler maintains segmented development and production environments, using technical and physical controls to limit network and application-level access to live systems. Employees have specific authorizations to access development and production systems.

(b) Zscaler utilizes a centralized log monitoring solution in combination with a SIEM to aggregate and correlate logged events.

(c) In order to protect against unauthorized access and modification, Zscaler captures network logs, OS-related logs, and intrusion detections.

(d) Zscaler identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never exceeded.

4. Ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control)

(a) All management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), Transport Layer Security (TLS) or Virtual Private Network (VPN) channels and remote access always requires multi-factor authentication.

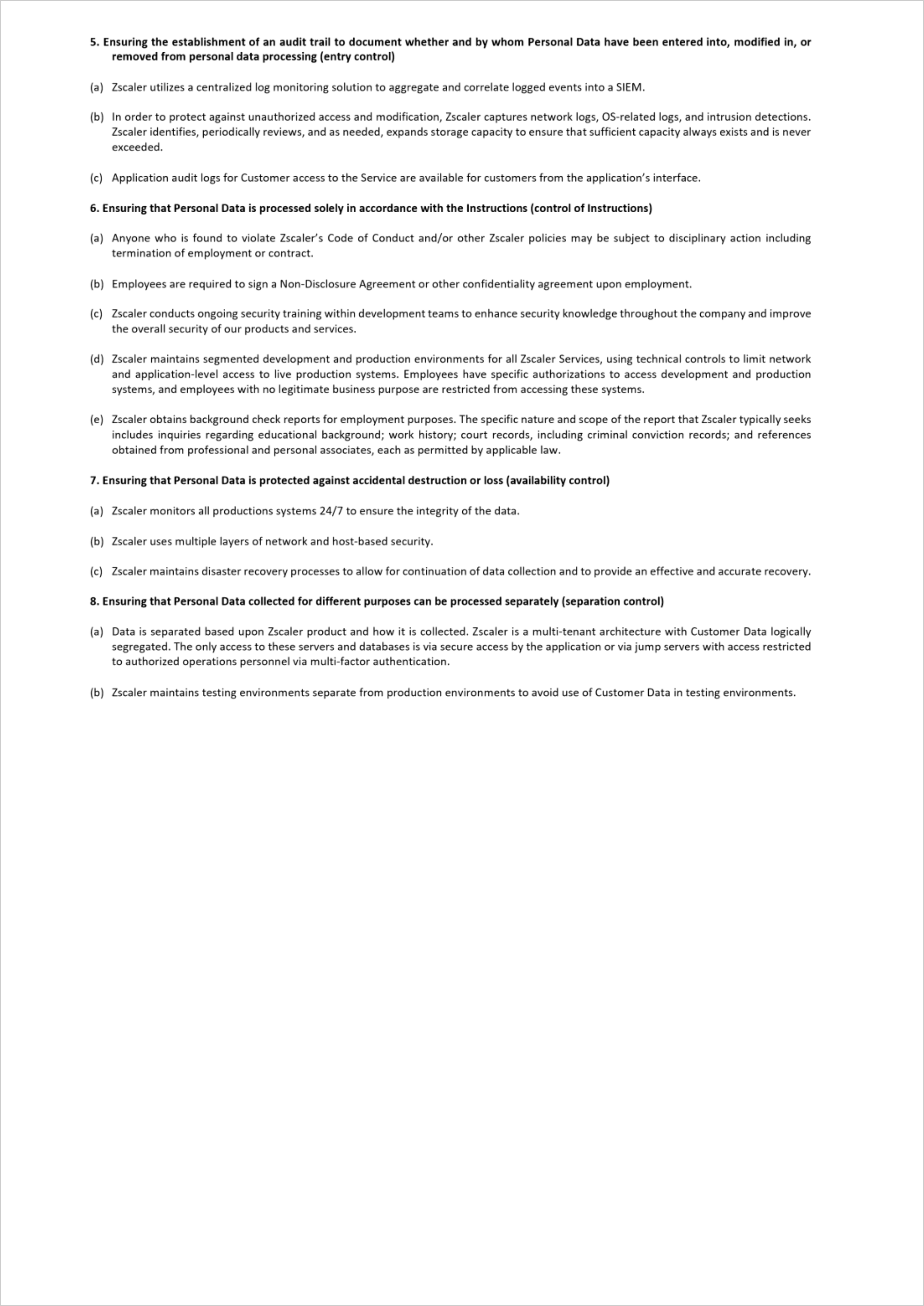
(b) Unless the connection originates from a list of trusted IP addresses, Zscaler does not allow management access from the Internet.

(c) Zscaler maintains a change management system to submit, authorize, and review any changes made in the production environment.

(d) Zscaler maintains a dedicated Network Operations Center (NOC), which is staffed 24/7.

Page 27

30 June 2020 14:55



5. Ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from personal data processing (entry control)

(a) Zscaler utilizes a centralized log monitoring solution to aggregate and correlate logged events into a SIEM.

(b) In order to protect against unauthorized access and modification, Zscaler captures network logs, OS-related logs, and intrusion detections. Zscaler identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never exceeded.

(c) Application audit logs for Customer access to the Service are available for customers from the application's interface.

6. Ensuring that Personal Data is processed solely in accordance with the Instructions (control of Instructions)

(a) Anyone who is found to violate Zscaler's Code of Conduct and/or other Zscaler policies may be subject to disciplinary action including termination of employment or contract.

(b) Employees are required to sign a Non-Disclosure Agreement or other confidentiality agreement upon employment.

(c) Zscaler conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services.

(d) Zscaler maintains segmented development and production environments for all Zscaler Services, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

(e) Zscaler obtains background check reports for employment purposes. The specific nature and scope of the report that Zscaler typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law.

7. Ensuring that Personal Data is protected against accidental destruction or loss (availability control)

(a) Zscaler monitors all productions systems 24/7 to ensure the integrity of the data.

(b) Zscaler uses multiple layers of network and host-based security.

(c) Zscaler maintains disaster recovery processes to allow for continuation of data collection and to provide an effective and accurate recovery.

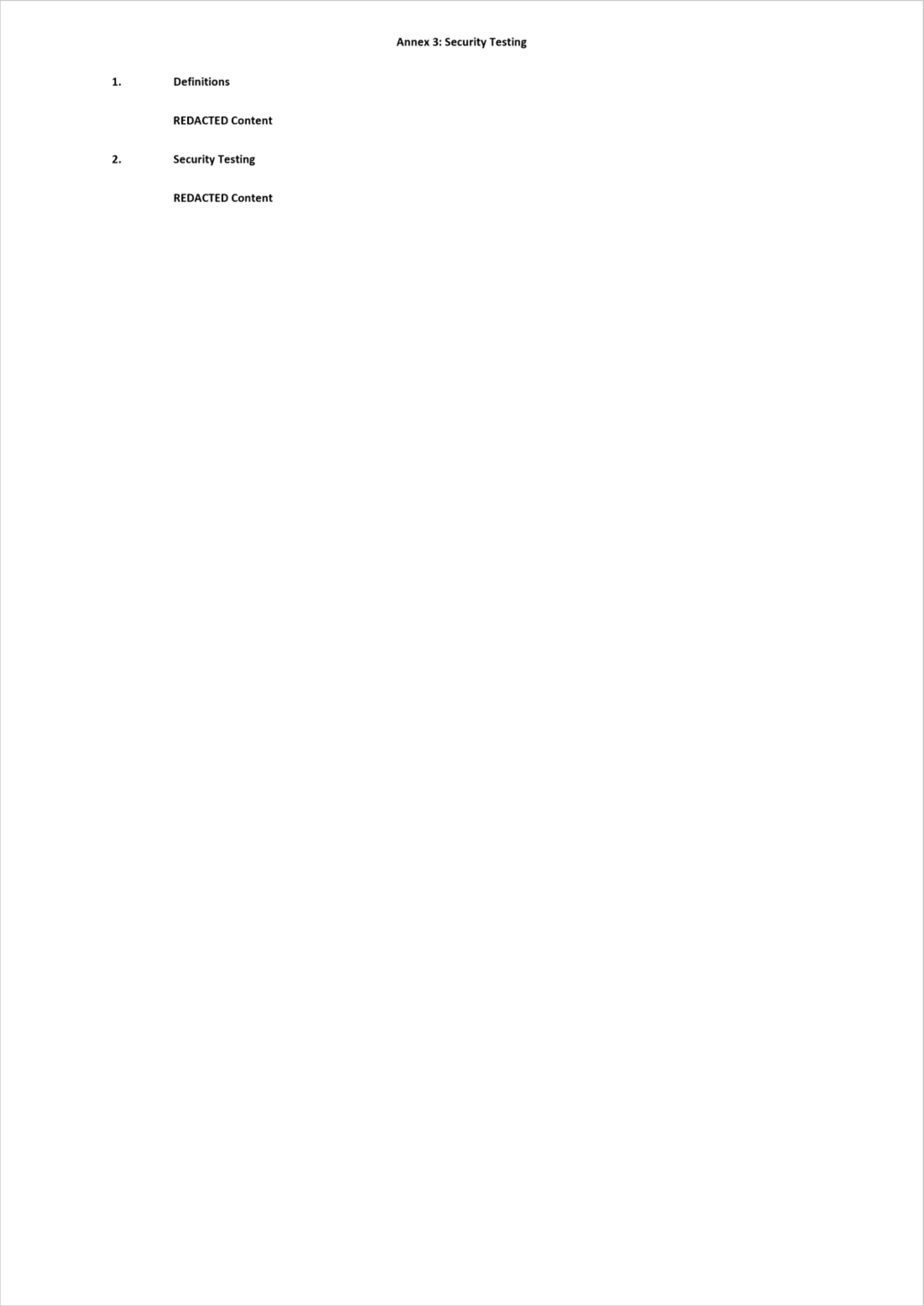
8. Ensuring that Personal Data collected for different purposes can be processed separately (separation control)

(a) Data is separated based upon Zscaler product and how it is collected. Zscaler is a multi-tenant architecture with Customer Data logically segregated. The only access to these servers and databases is via secure access by the application or via jump servers with access restricted to authorized operations personnel via multi-factor authentication.

(b) Zscaler maintains testing environments separate from production environments to avoid use of Customer Data in testing environments.

Page 28

30 June 2020 14:55



Annex 3: Security Testing

1. **Definitions**

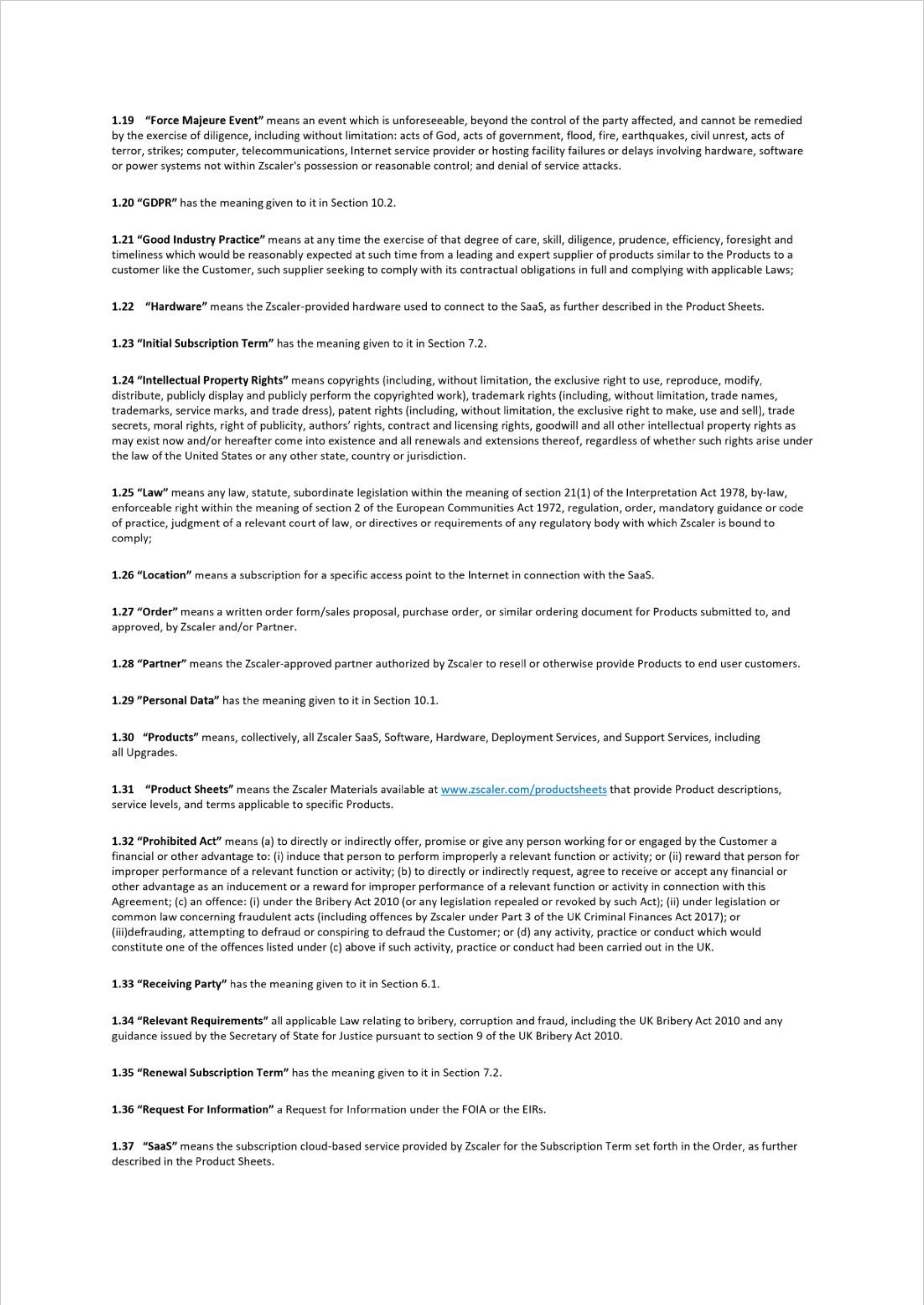
   REDACTED Content

2. **Security Testing**

   REDACTED Content

Page 2

30 June 2020 14:51



1.19 "Force Majeure Event" means an event which is unforeseeable, beyond the control of the party affected, and cannot be remedied by the exercise of diligence, including without limitation: acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes; computer, telecommunications, Internet service provider or hosting facility failures or delays involving hardware, software or power systems not within Zscaler's possession or reasonable control; and denial of service attacks.

1.20 "GDPR" has the meaning given to it in Section 10.2.

1.21 "Good Industry Practice" means at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of products similar to the Products to a customer like the Customer, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws;

1.22 "Hardware" means the Zscaler-provided hardware used to connect to the SaaS, as further described in the Product Sheets.

1.23 "Initial Subscription Term" has the meaning given to it in Section 7.2.

1.24 "Intellectual Property Rights" means copyrights (including, without limitation, the exclusive right to use, reproduce, modify, distribute, publicly display and publicly perform the copyrighted work), trademark rights (including, without limitation, trade names, trademarks, service marks, and trade dress), patent rights (including, without limitation, the exclusive right to make, use and sell), trade secrets, moral rights, right of publicity, authors' rights, contract and licensing rights, goodwill and all other intellectual property rights as may exist now and/or hereafter come into existence and all renewals and extensions thereof, regardless of whether such rights arise under the law of the United States or any other state, country or jurisdiction.

1.25 "Law" means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, by-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which Zscaler is bound to comply;

1.26 "Location" means a subscription for a specific access point to the Internet in connection with the SaaS.

1.27 "Order" means a written order form/sales proposal, purchase order, or similar ordering document for Products submitted to, and approved, by Zscaler and/or Partner.

1.28 "Partner" means the Zscaler-approved partner authorized by Zscaler to resell or otherwise provide Products to end user customers.

1.29 "Personal Data" has the meaning given to it in Section 10.1.

1.30 "Products" means, collectively, all Zscaler SaaS, Software, Hardware, Deployment Services, and Support Services, including all Upgrades.

1.31 "Product Sheets" means the Zscaler Materials available at www.zscaler.com/productsheets that provide Product descriptions, service levels, and terms applicable to specific Products.

1.32 "Prohibited Act" means (a) to directly or indirectly offer, promise or give any person working for or engaged by the Customer a financial or other advantage to: (i) induce that person to perform improperly a relevant function or activity; or (ii) reward that person for improper performance of a relevant function or activity; (b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Agreement; (c) an offence: (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); (ii) under legislation or common law concerning fraudulent acts (including offences by Zscaler under Part 3 of the UK Criminal Finances Act 2017); or (iii)defrauding, attempting to defraud or conspiring to defraud the Customer; or (d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK.

1.33 "Receiving Party" has the meaning given to it in Section 6.1.

1.34 "Relevant Requirements" all applicable Law relating to bribery, corruption and fraud, including the UK Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the UK Bribery Act 2010.

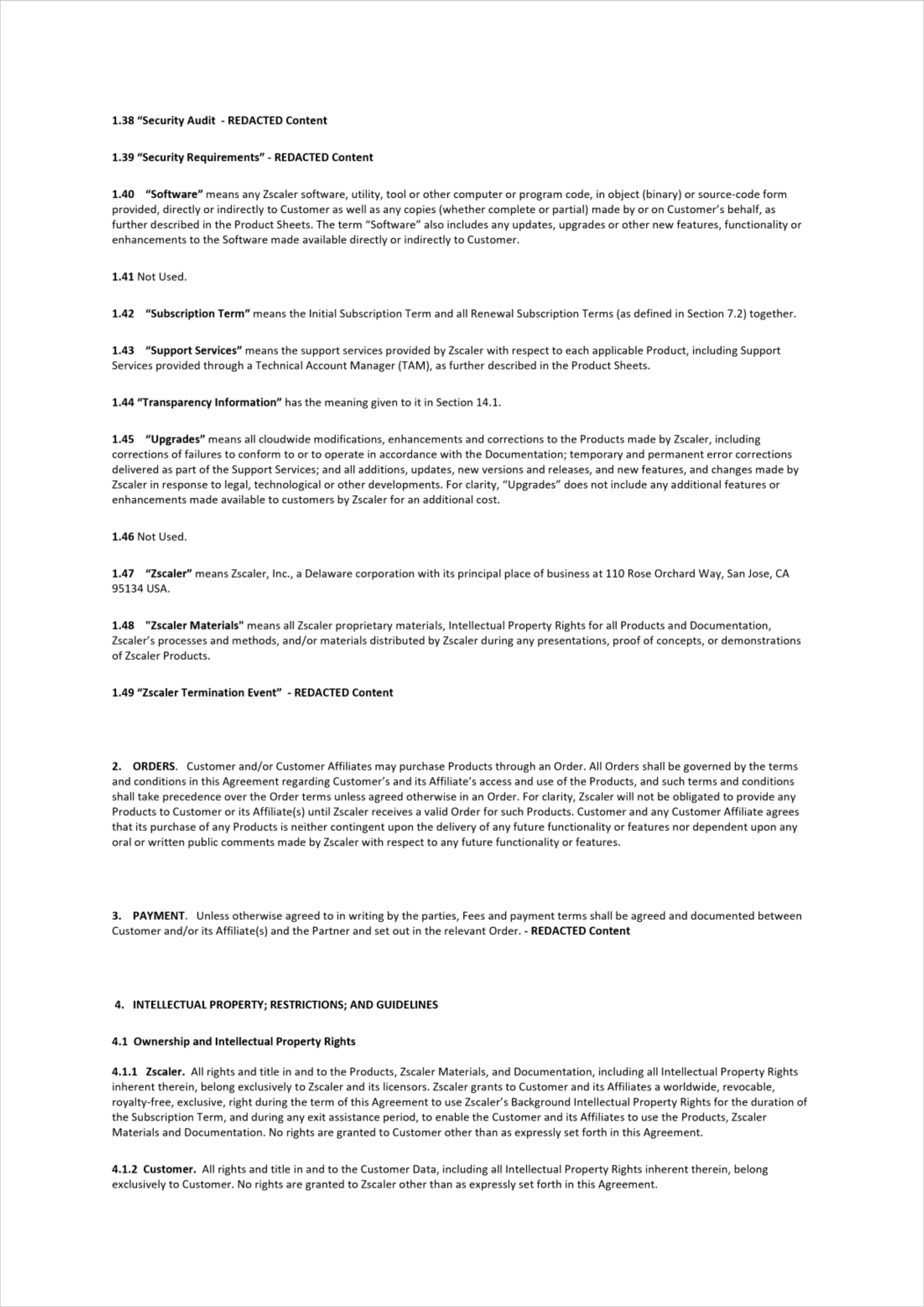
1.35 "Renewal Subscription Term" has the meaning given to it in Section 7.2.

1.36 "Request For Information" a Request for Information under the FOIA or the EIRs.

1.37 "SaaS" means the subscription cloud-based service provided by Zscaler for the Subscription Term set forth in the Order, as further described in the Product Sheets.

Page 3

30 June 2020 14:51



1.38 “Security Audit - REDACTED Content

1.39 “Security Requirements” - REDACTED Content

1.40 “Software” means any Zscaler software, utility, tool or other computer or program code, in object (binary) or source-code form provided, directly or indirectly to Customer as well as any copies (whether complete or partial) made by or on Customer’s behalf, as further described in the Product Sheets. The term “Software” also includes any updates, upgrades or other new features, functionality or enhancements to the Software made available directly or indirectly to Customer.

1.41 Not Used.

1.42 “Subscription Term” means the Initial Subscription Term and all Renewal Subscription Terms (as defined in Section 7.2) together.

1.43 “Support Services” means the support services provided by Zscaler with respect to each applicable Product, including Support Services provided through a Technical Account Manager (TAM), as further described in the Product Sheets.

1.44 “Transparency Information” has the meaning given to it in Section 14.1.

1.45 “Upgrades” means all cloudwide modifications, enhancements and corrections to the Products made by Zscaler, including corrections of failures to conform to or to operate in accordance with the Documentation; temporary and permanent error corrections delivered as part of the Support Services; and all additions, updates, new versions and releases, and new features, and changes made by Zscaler in response to legal, technological or other developments. For clarity, “Upgrades” does not include any additional features or enhancements made available to customers by Zscaler for an additional cost.

1.46 Not Used.

1.47 “Zscaler” means Zscaler, Inc., a Delaware corporation with its principal place of business at 110 Rose Orchard Way, San Jose, CA 95134 USA.

1.48 "Zscaler Materials" means all Zscaler proprietary materials, Intellectual Property Rights for all Products and Documentation, Zscaler’s processes and methods, and/or materials distributed by Zscaler during any presentations, proof of concepts, or demonstrations of Zscaler Products.

1.49 “Zscaler Termination Event” - REDACTED Content

2. ORDERS. Customer and/or Customer Affiliates may purchase Products through an Order. All Orders shall be governed by the terms and conditions in this Agreement regarding Customer’s and its Affiliate’s access and use of the Products, and such terms and conditions shall take precedence over the Order terms unless agreed otherwise in an Order. For clarity, Zscaler will not be obligated to provide any Products to Customer or its Affiliate(s) until Zscaler receives a valid Order for such Products. Customer and any Customer Affiliate agrees that its purchase of any Products is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written public comments made by Zscaler with respect to any future functionality or features.

3. PAYMENT. Unless otherwise agreed to in writing by the parties, Fees and payment terms shall be agreed and documented between Customer and/or its Affiliate(s) and the Partner and set out in the relevant Order. **- REDACTED Content**

4. INTELLECTUAL PROPERTY; RESTRICTIONS; AND GUIDELINES

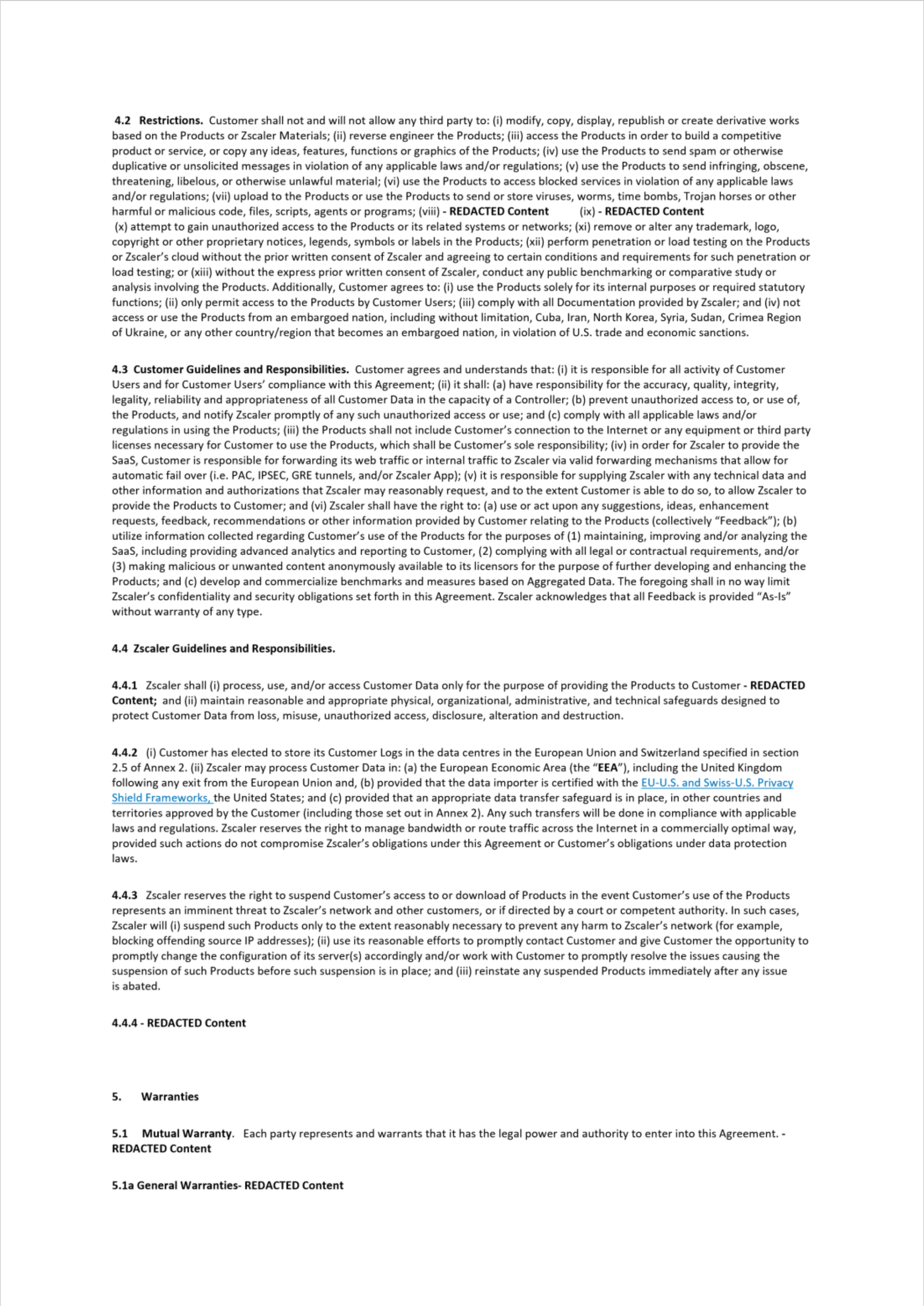
4.1 Ownership and Intellectual Property Rights

4.1.1 Zscaler. All rights and title in and to the Products, Zscaler Materials, and Documentation, including all Intellectual Property Rights inherent therein, belong exclusively to Zscaler and its licensors. Zscaler grants to Customer and its Affiliates a worldwide, revocable, royalty-free, exclusive, right during the term of this Agreement to use Zscaler’s Background Intellectual Property Rights for the duration of the Subscription Term, and during any exit assistance period, to enable the Customer and its Affiliates to use the Products, Zscaler Materials and Documentation. No rights are granted to Customer other than as expressly set forth in this Agreement.

4.1.2 Customer. All rights and title in and to the Customer Data, including all Intellectual Property Rights inherent therein, belong exclusively to Customer. No rights are granted to Zscaler other than as expressly set forth in this Agreement.

Page 4

30 June 2020 14:51



4.2 Restrictions. Customer shall not and will not allow any third party to: (i) modify, copy, display, republish or create derivative works based on the Products or Zscaler Materials; (ii) reverse engineer the Products; (iii) access the Products in order to build a competitive product or service, or copy any ideas, features, functions or graphics of the Products; (iv) use the Products to send spam or otherwise duplicative or unsolicited messages in violation of any applicable laws and/or regulations; (v) use the Products to send infringing, obscene, threatening, libelous, or otherwise unlawful material; (vi) use the Products to access blocked services in violation of any applicable laws and/or regulations; (vii) upload to the Products or use the Products to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs; (viii) **- REDACTED Content** (ix) **- REDACTED Content** (x) attempt to gain unauthorized access to the Products or its related systems or networks; (xi) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Products; (xii) perform penetration or load testing on the Products or Zscaler's cloud without the prior written consent of Zscaler and agreeing to certain conditions and requirements for such penetration or load testing; or (xiii) without the express prior written consent of Zscaler, conduct any public benchmarking or comparative study or analysis involving the Products. Additionally, Customer agrees to: (i) use the Products solely for its internal purposes or required statutory functions; (ii) only permit access to the Products by Customer Users; (iii) comply with all Documentation provided by Zscaler; and (iv) not access or use the Products from an embargoed nation, including without limitation, Cuba, Iran, North Korea, Syria, Sudan, Crimea Region of Ukraine, or any other country/region that becomes an embargoed nation, in violation of U.S. trade and economic sanctions.

4.3 Customer Guidelines and Responsibilities. Customer agrees and understands that: (i) it is responsible for all activity of Customer Users and for Customer Users' compliance with this Agreement; (ii) it shall: (a) have responsibility for the accuracy, quality, integrity, legality, reliability and appropriateness of all Customer Data in the capacity of a Controller; (b) prevent unauthorized access to, or use of, the Products, and notify Zscaler promptly of any such unauthorized access or use; and (c) comply with all applicable laws and/or regulations in using the Products; (iii) the Products shall not include Customer's connection to the Internet or any equipment or third party licenses necessary for Customer to use the Products, which shall be Customer's sole responsibility; (iv) in order for Zscaler to provide the SaaS, Customer is responsible for forwarding its web traffic or internal traffic to Zscaler via valid forwarding mechanisms that allow for automatic fail over (i.e. PAC, IPSEC, GRE tunnels, and/or Zscaler App); (v) it is responsible for supplying Zscaler with any technical data and other information and authorizations that Zscaler may reasonably request, and to the extent Customer is able to do so, to allow Zscaler to provide the Products to Customer; and (vi) Zscaler shall have the right to: (a) use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer relating to the Products (collectively "Feedback"); (b) utilize information collected regarding Customer's use of the Products for the purposes of (1) maintaining, improving and/or analyzing the SaaS, including providing advanced analytics and reporting to Customer, (2) complying with all legal or contractual requirements, and/or (3) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Products; and (c) develop and commercialize benchmarks and measures based on Aggregated Data. The foregoing shall in no way limit Zscaler's confidentiality and security obligations set forth in this Agreement. Zscaler acknowledges that all Feedback is provided "As-Is" without warranty of any type.

4.4 Zscaler Guidelines and Responsibilities.

4.4.1 Zscaler shall (i) process, use, and/or access Customer Data only for the purpose of providing the Products to Customer **- REDACTED Content;** and (ii) maintain reasonable and appropriate physical, organizational, administrative, and technical safeguards designed to protect Customer Data from loss, misuse, unauthorized access, disclosure, alteration and destruction.

4.4.2 (i) Customer has elected to store its Customer Logs in the data centres in the European Union and Switzerland specified in section 2.5 of Annex 2. (ii) Zscaler may process Customer Data in: (a) the European Economic Area (the "**EEA**"), including the United Kingdom following any exit from the European Union and, (b) provided that the data importer is certified with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, the United States; and (c) provided that an appropriate data transfer safeguard is in place, in other countries and territories approved by the Customer (including those set out in Annex 2). Any such transfers will be done in compliance with applicable laws and regulations. Zscaler reserves the right to manage bandwidth or route traffic across the Internet in a commercially optimal way, provided such actions do not compromise Zscaler's obligations under this Agreement or Customer's obligations under data protection laws.

4.4.3 Zscaler reserves the right to suspend Customer's access to or download of Products in the event Customer's use of the Products represents an imminent threat to Zscaler's network and other customers, or if directed by a court or competent authority. In such cases, Zscaler will (i) suspend such Products only to the extent reasonably necessary to prevent any harm to Zscaler's network (for example, blocking offending source IP addresses); (ii) use its reasonable efforts to promptly contact Customer and give Customer the opportunity to promptly change the configuration of its server(s) accordingly and/or work with Customer to promptly resolve the issues causing the suspension of such Products before such suspension is in place; and (iii) reinstate any suspended Products immediately after any issue is abated.

4.4.4 - REDACTED Content

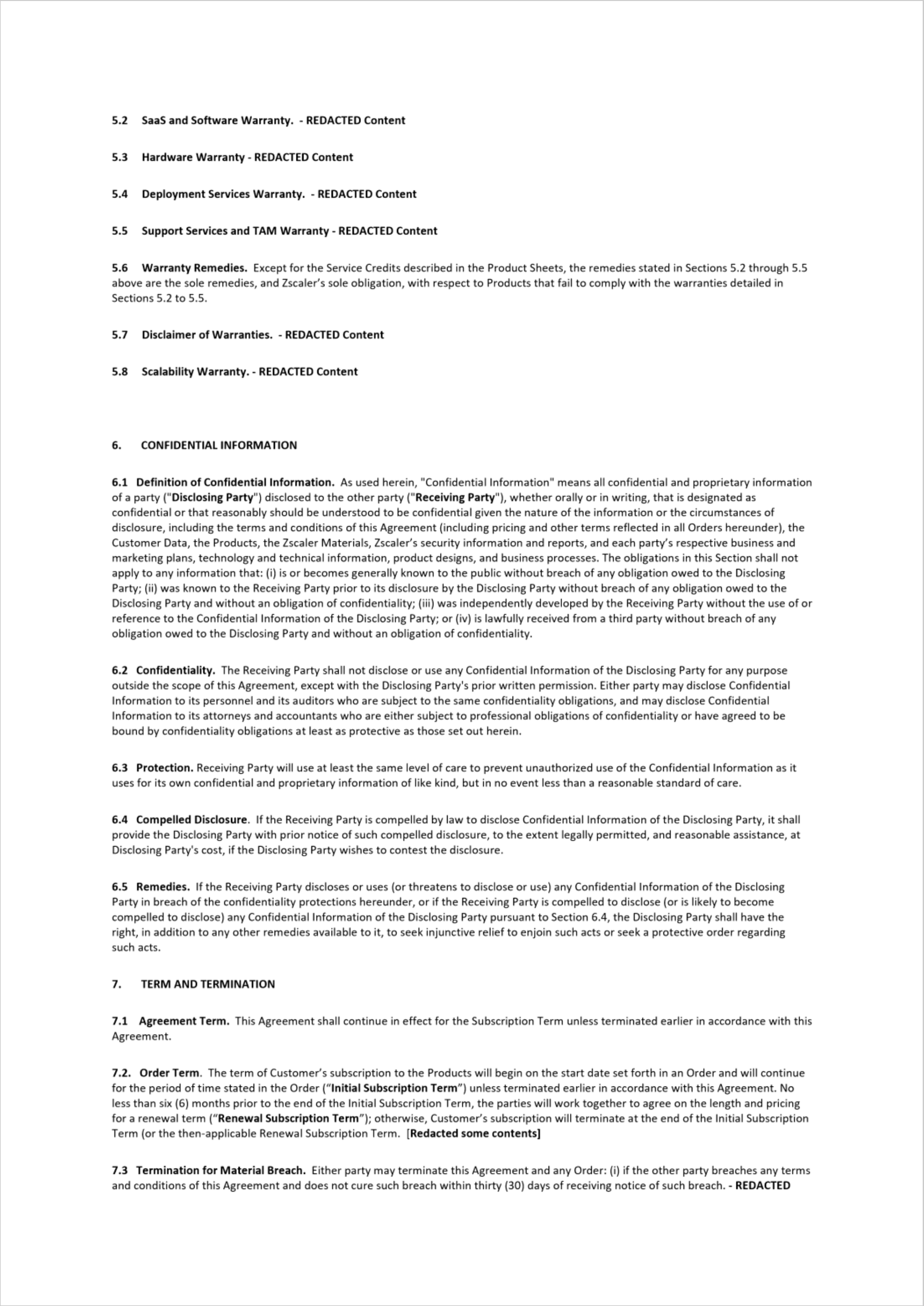
5. Warranties

5.1 Mutual Warranty. Each party represents and warrants that it has the legal power and authority to enter into this Agreement. **- REDACTED Content**

5.1a General Warranties- REDACTED Content

Page 5

30 June 2020 14:51



5.2 SaaS and Software Warranty. - REDACTED Content

5.3 Hardware Warranty - REDACTED Content

5.4 Deployment Services Warranty. - REDACTED Content

5.5 Support Services and TAM Warranty - REDACTED Content

5.6 Warranty Remedies. Except for the Service Credits described in the Product Sheets, the remedies stated in Sections 5.2 through 5.5 above are the sole remedies, and Zscaler's sole obligation, with respect to Products that fail to comply with the warranties detailed in Sections 5.2 to 5.5.

5.7 Disclaimer of Warranties. - REDACTED Content

5.8 Scalability Warranty. - REDACTED Content

6. CONFIDENTIAL INFORMATION

6.1 Definition of Confidential Information. As used herein, "Confidential Information" means all confidential and proprietary information of a party ("**Disclosing Party**") disclosed to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information or the circumstances of disclosure, including the terms and conditions of this Agreement (including pricing and other terms reflected in all Orders hereunder), the Customer Data, the Products, the Zscaler Materials, Zscaler's security information and reports, and each party's respective business and marketing plans, technology and technical information, product designs, and business processes. The obligations in this Section shall not apply to any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party and without an obligation of confidentiality; (iii) was independently developed by the Receiving Party without the use of or reference to the Confidential Information of the Disclosing Party; or (iv) is lawfully received from a third party without breach of any obligation owed to the Disclosing Party and without an obligation of confidentiality.

6.2 Confidentiality. The Receiving Party shall not disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, except with the Disclosing Party's prior written permission. Either party may disclose Confidential Information to its personnel and its auditors who are subject to the same confidentiality obligations, and may disclose Confidential Information to its attorneys and accountants who are either subject to professional obligations of confidentiality or have agreed to be bound by confidentiality obligations at least as protective as those set out herein.

6.3 Protection. Receiving Party will use at least the same level of care to prevent unauthorized use of the Confidential Information as it uses for its own confidential and proprietary information of like kind, but in no event less than a reasonable standard of care.

6.4 Compelled Disclosure. If the Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of such compelled disclosure, to the extent legally permitted, and reasonable assistance, at Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

6.5 Remedies. If the Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the Disclosing Party in breach of the confidentiality protections hereunder, or if the Receiving Party is compelled to disclose (or is likely to become compelled to disclose) any Confidential Information of the Disclosing Party pursuant to Section 6.4, the Disclosing Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts or seek a protective order regarding such acts.

7. TERM AND TERMINATION

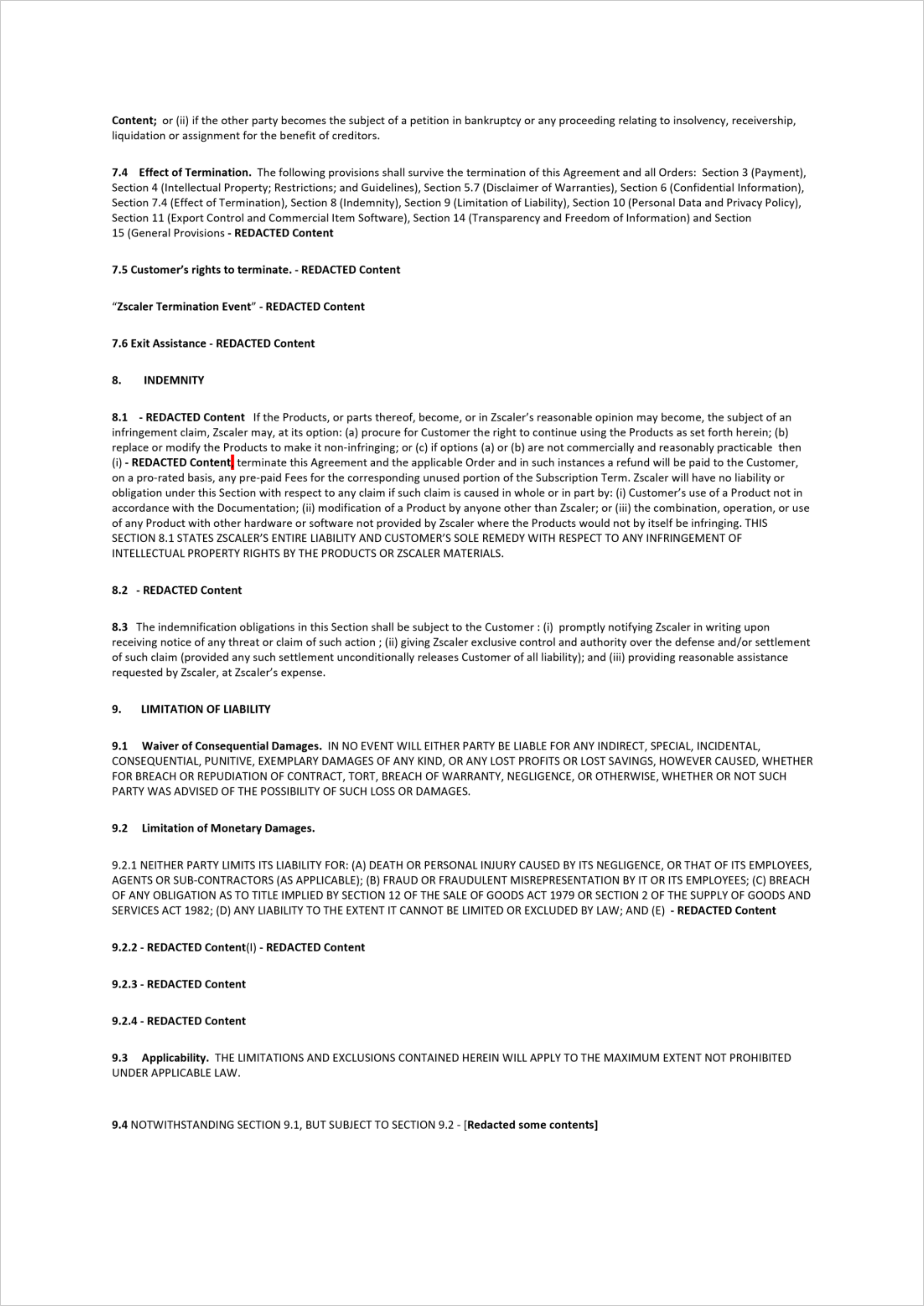
7.1 Agreement Term. This Agreement shall continue in effect for the Subscription Term unless terminated earlier in accordance with this Agreement.

7.2. Order Term. The term of Customer's subscription to the Products will begin on the start date set forth in an Order and will continue for the period of time stated in the Order ("**Initial Subscription Term**") unless terminated earlier in accordance with this Agreement. No less than six (6) months prior to the end of the Initial Subscription Term, the parties will work together to agree on the length and pricing for a renewal term ("**Renewal Subscription Term**"); otherwise, Customer's subscription will terminate at the end of the Initial Subscription Term (or the then-applicable Renewal Subscription Term. [**Redacted some contents]**

7.3 Termination for Material Breach. Either party may terminate this Agreement and any Order: (i) if the other party breaches any terms and conditions of this Agreement and does not cure such breach within thirty (30) days of receiving notice of such breach. - **REDACTED**

Page 6

30 June 2020 14:51



Content; or (ii) if the other party becomes the subject of a petition in bankruptcy or any proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

7.4 Effect of Termination. The following provisions shall survive the termination of this Agreement and all Orders: Section 3 (Payment), Section 4 (Intellectual Property; Restrictions; and Guidelines), Section 5.7 (Disclaimer of Warranties), Section 6 (Confidential Information), Section 7.4 (Effect of Termination), Section 8 (Indemnity), Section 9 (Limitation of Liability), Section 10 (Personal Data and Privacy Policy), Section 11 (Export Control and Commercial Item Software), Section 14 (Transparency and Freedom of Information) and Section 15 (General Provisions **- REDACTED Content**

7.5 Customer's rights to terminate. - REDACTED Content

"Zscaler Termination Event" - REDACTED Content

7.6 Exit Assistance - REDACTED Content

8. INDEMNITY

8.1 - REDACTED Content If the Products, or parts thereof, become, or in Zscaler's reasonable opinion may become, the subject of an infringement claim, Zscaler may, at its option: (a) procure for Customer the right to continue using the Products as set forth herein; (b) replace or modify the Products to make it non-infringing; or (c) if options (a) or (b) are not commercially and reasonably practicable then (i) **- REDACTED Content** terminate this Agreement and the applicable Order and in such instances a refund will be paid to the Customer, on a pro-rated basis, any pre-paid Fees for the corresponding unused portion of the Subscription Term. Zscaler will have no liability or obligation under this Section with respect to any claim if such claim is caused in whole or in part by: (i) Customer's use of a Product not in accordance with the Documentation; (ii) modification of a Product by anyone other than Zscaler; or (iii) the combination, operation, or use of any Product with other hardware or software not provided by Zscaler where the Products would not by itself be infringing. THIS SECTION 8.1 STATES ZSCALER'S ENTIRE LIABILITY AND CUSTOMER'S SOLE REMEDY WITH RESPECT TO ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS BY THE PRODUCTS OR ZSCALER MATERIALS.

8.2 - REDACTED Content

8.3 The indemnification obligations in this Section shall be subject to the Customer : (i) promptly notifying Zscaler in writing upon receiving notice of any threat or claim of such action ; (ii) giving Zscaler exclusive control and authority over the defense and/or settlement of such claim (provided any such settlement unconditionally releases Customer of all liability); and (iii) providing reasonable assistance requested by Zscaler, at Zscaler's expense.

9. LIMITATION OF LIABILITY

9.1 Waiver of Consequential Damages. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY DAMAGES OF ANY KIND, OR ANY LOST PROFITS OR LOST SAVINGS, HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT SUCH PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

9.2 Limitation of Monetary Damages.

9.2.1 NEITHER PARTY LIMITS ITS LIABILITY FOR: (A) DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE, OR THAT OF ITS EMPLOYEES, AGENTS OR SUB-CONTRACTORS (AS APPLICABLE); (B) FRAUD OR FRAUDULENT MISREPRESENTATION BY IT OR ITS EMPLOYEES; (C) BREACH OF ANY OBLIGATION AS TO TITLE IMPLIED BY SECTION 12 OF THE SALE OF GOODS ACT 1979 OR SECTION 2 OF THE SUPPLY OF GOODS AND SERVICES ACT 1982; (D) ANY LIABILITY TO THE EXTENT IT CANNOT BE LIMITED OR EXCLUDED BY LAW; AND (E) **- REDACTED Content**

9.2.2 - REDACTED Content(I) **- REDACTED Content**

9.2.3 - REDACTED Content

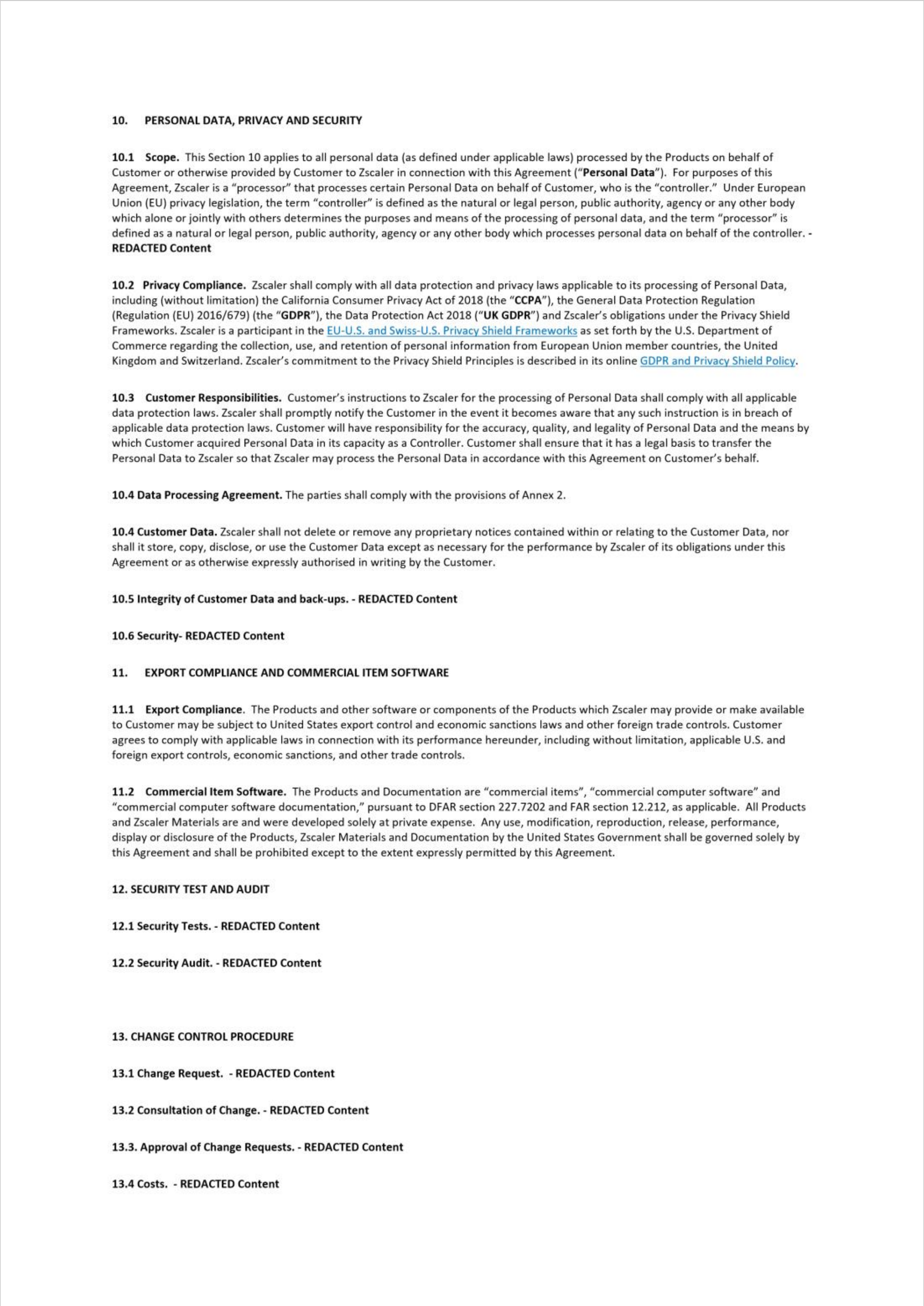
9.2.4 - REDACTED Content

9.3 Applicability. THE LIMITATIONS AND EXCLUSIONS CONTAINED HEREIN WILL APPLY TO THE MAXIMUM EXTENT NOT PROHIBITED UNDER APPLICABLE LAW.

9.4 NOTWITHSTANDING SECTION 9.1, BUT SUBJECT TO SECTION 9.2 - [**Redacted some contents]**

Page 7

30 June 2020 14:51



10. PERSONAL DATA, PRIVACY AND SECURITY

10.1 Scope. This Section 10 applies to all personal data (as defined under applicable laws) processed by the Products on behalf of Customer or otherwise provided by Customer to Zscaler in connection with this Agreement ("**Personal Data**"). For purposes of this Agreement, Zscaler is a "processor" that processes certain Personal Data on behalf of Customer, who is the "controller." Under European Union (EU) privacy legislation, the term "controller" is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, and the term "processor" is defined as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. - **REDACTED Content**

10.2 Privacy Compliance. Zscaler shall comply with all data protection and privacy laws applicable to its processing of Personal Data, including (without limitation) the California Consumer Privacy Act of 2018 (the "**CCPA**"), the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"), the Data Protection Act 2018 ("**UK GDPR**") and Zscaler's obligations under the Privacy Shield Frameworks. Zscaler is a participant in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries, the United Kingdom and Switzerland. Zscaler's commitment to the Privacy Shield Principles is described in its online GDPR and Privacy Shield Policy.

10.3 Customer Responsibilities. Customer's instructions to Zscaler for the processing of Personal Data shall comply with all applicable data protection laws. Zscaler shall promptly notify the Customer in the event it becomes aware that any such instruction is in breach of applicable data protection laws. Customer will have responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data in its capacity as a Controller. Customer shall ensure that it has a legal basis to transfer the Personal Data to Zscaler so that Zscaler may process the Personal Data in accordance with this Agreement on Customer's behalf.

10.4 Data Processing Agreement. The parties shall comply with the provisions of Annex 2.

10.4 Customer Data. Zscaler shall not delete or remove any proprietary notices contained within or relating to the Customer Data, nor shall it store, copy, disclose, or use the Customer Data except as necessary for the performance by Zscaler of its obligations under this Agreement or as otherwise expressly authorised in writing by the Customer.

10.5 Integrity of Customer Data and back-ups. - REDACTED Content

10.6 Security- REDACTED Content

11. EXPORT COMPLIANCE AND COMMERCIAL ITEM SOFTWARE

11.1 Export Compliance. The Products and other software or components of the Products which Zscaler may provide or make available to Customer may be subject to United States export control and economic sanctions laws and other foreign trade controls. Customer agrees to comply with applicable laws in connection with its performance hereunder, including without limitation, applicable U.S. and foreign export controls, economic sanctions, and other trade controls.

11.2 Commercial Item Software. The Products and Documentation are "commercial items", "commercial computer software" and "commercial computer software documentation," pursuant to DFAR section 227.7202 and FAR section 12.212, as applicable. All Products and Zscaler Materials are and were developed solely at private expense. Any use, modification, reproduction, release, performance, display or disclosure of the Products, Zscaler Materials and Documentation by the United States Government shall be governed solely by this Agreement and shall be prohibited except to the extent expressly permitted by this Agreement.

12. SECURITY TEST AND AUDIT

12.1 Security Tests. - REDACTED Content

12.2 Security Audit. - REDACTED Content

13. CHANGE CONTROL PROCEDURE

13.1 Change Request. - REDACTED Content

13.2 Consultation of Change. - REDACTED Content

13.3. Approval of Change Requests. - REDACTED Content

13.4 Costs. - REDACTED Content

Page 8

30 June 2020 14:51

14. TRANSPARENCY AND FREEDOM OF INFORMATION

14.1. Transparency Information. The Parties acknowledge that the content of this Agreement, including any changes to this Agreement agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Customer; and (ii) commercially sensitive information (together the "**Transparency Information**") are not Confidential Information. Notwithstanding any other provision of this Agreement, Zscaler hereby gives its consent for the Customer to publish to the general public the Transparency Information in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted).

14.2. Redactions. The Customer shall, prior to publication, consult with Zscaler on the manner and format of publication and to inform its decision regarding any redactions but shall have the final decision in its absolute discretion.

14.3. Assistance. Zscaler shall assist and co-operate with the Customer to enable the Customer to publish the Transparency Information.

14.4. Public Interest. If the Customer believes that publication of any element of the Transparency Information would be contrary to the public interest, the Customer shall be entitled to exclude such information from publication. The Customer acknowledges that it would expect the public interest by default to be best served by publication of the Transparency Information in its entirety. Accordingly, the Customer acknowledges that it will only exclude Transparency Information from publication in exceptional circumstances and agrees that where it decides to exclude information from publication it will provide a clear explanation to Zscaler.

14.5. Publication. The Customer shall publish the Transparency Information in a format that assists the general public in understanding the relevance and completeness of the information being published to ensure the public obtain a fair view on how the Agreement is being performed, having regard to the context of the wider commercial relationship with Zscaler. Zscaler shall provide to the Customer within 5 business days (or such other period as the Customer may reasonably specify) any such Information requested by the Customer.

14.5. EIRS and FOIA. Zscaler acknowledges that the Customer is subject to the requirements of the FOIA and the EIRs. Zscaler shall: (a) provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and EIRs; (b) transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 business days of receipt; (c) provide the Customer with a copy of all Information held on behalf of the Customer which is requested in a Request For Information and which is in its possession or control in the form that the Customer requires within 5 business days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and (d) not respond directly to a Request For Information addressed to the Customer unless authorised in writing to do so by the Customer. Zscaler acknowledges that the Customer may be required under the FOIA and EIRs to disclose Information (including commercially sensitive information) without consulting or obtaining consent from Zscaler. The Customer shall take reasonable steps to notify Zscaler of a Request For Information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Agreement) the Customer shall be responsible for determining in its absolute discretion whether any commercially sensitive information and/or any other information is exempt from disclosure in accordance with the FOIA and EIRs.

15. GENERAL PROVISIONS

15.1 Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties.

15.2 Notices. All notices required to be sent hereunder shall be in writing or via e-mail, addressed to receiving party's current business contact, if known, with a cc: to the Legal Department of the receiving party, and sent to the party's address as listed in the Order, or as updated by either party by written notice. Notices shall be effective upon receipt and shall be deemed to be received as follows: (i) if personally delivered by courier, when delivered; or (ii) if mailed by first class mail, or the local equivalent, on the fifth business day after posting with the proper address; or (iii) if sent via email 9.00am on the first business day after sending.

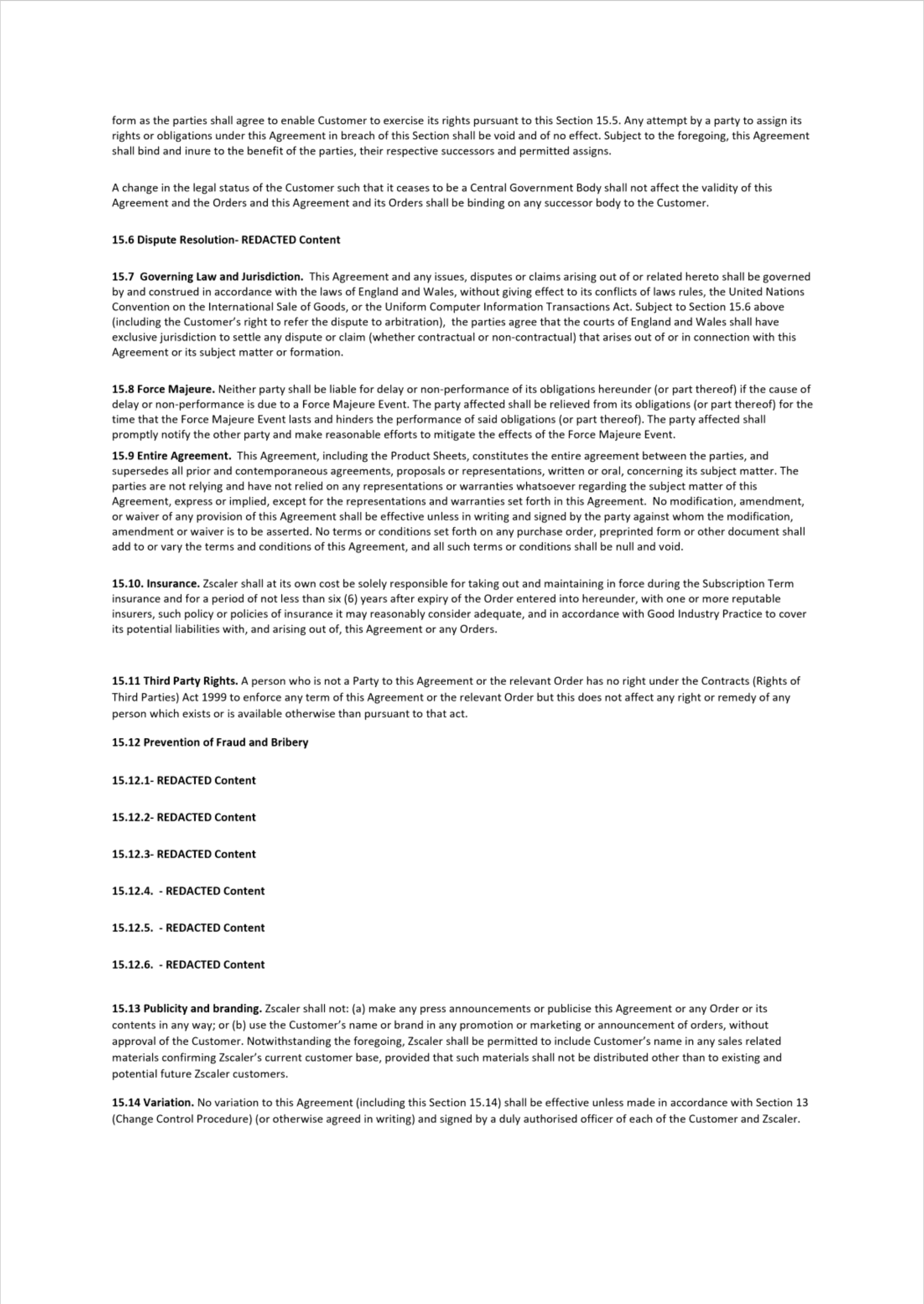
15.3 Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

15.4 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in full force and effect.

15.5 Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld), except that: (A) either party may assign this Agreement in its entirety, without the consent of the other party, to: (i) an Affiliate; or (ii) in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party; and (B) the Customer may at its discretion assign or novate all of its rights, obligations and liabilities under this Agreement or any Order and/or any associated licences to a body other than a Central Government Body (but not include any private sector body) which performs any of the functions that previously had been performed by the Customer, and Zscaler shall at Customer's request, enter into a novation agreement in such

Page 9

30 June 2020 14:51



form as the parties shall agree to enable Customer to exercise its rights pursuant to this Section 15.5. Any attempt by a party to assign its rights or obligations under this Agreement in breach of this Section shall be void and of no effect. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

A change in the legal status of the Customer such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and the Orders and this Agreement and its Orders shall be binding on any successor body to the Customer.

15.6 Dispute Resolution- REDACTED Content

15.7 Governing Law and Jurisdiction. This Agreement and any issues, disputes or claims arising out of or related hereto shall be governed by and construed in accordance with the laws of England and Wales, without giving effect to its conflicts of laws rules, the United Nations Convention on the International Sale of Goods, or the Uniform Computer Information Transactions Act. Subject to Section 15.6 above (including the Customer's right to refer the dispute to arbitration), the parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

15.8 Force Majeure. Neither party shall be liable for delay or non-performance of its obligations hereunder (or part thereof) if the cause of delay or non-performance is due to a Force Majeure Event. The party affected shall be relieved from its obligations (or part thereof) for the time that the Force Majeure Event lasts and hinders the performance of said obligations (or part thereof). The party affected shall promptly notify the other party and make reasonable efforts to mitigate the effects of the Force Majeure Event.

15.9 Entire Agreement. This Agreement, including the Product Sheets, constitutes the entire agreement between the parties, and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. The parties are not relying and have not relied on any representations or warranties whatsoever regarding the subject matter of this Agreement, express or implied, except for the representations and warranties set forth in this Agreement. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. No terms or conditions set forth on any purchase order, preprinted form or other document shall add to or vary the terms and conditions of this Agreement, and all such terms or conditions shall be null and void.

15.10. Insurance. Zscaler shall at its own cost be solely responsible for taking out and maintaining in force during the Subscription Term insurance and for a period of not less than six (6) years after expiry of the Order entered into hereunder, with one or more reputable insurers, such policy or policies of insurance it may reasonably consider adequate, and in accordance with Good Industry Practice to cover its potential liabilities with, and arising out of, this Agreement or any Orders.

15.11 Third Party Rights. A person who is not a Party to this Agreement or the relevant Order has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement or the relevant Order but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that act.

15.12 Prevention of Fraud and Bribery

15.12.1- REDACTED Content

15.12.2- REDACTED Content

15.12.3- REDACTED Content

15.12.4. - REDACTED Content

15.12.5. - REDACTED Content

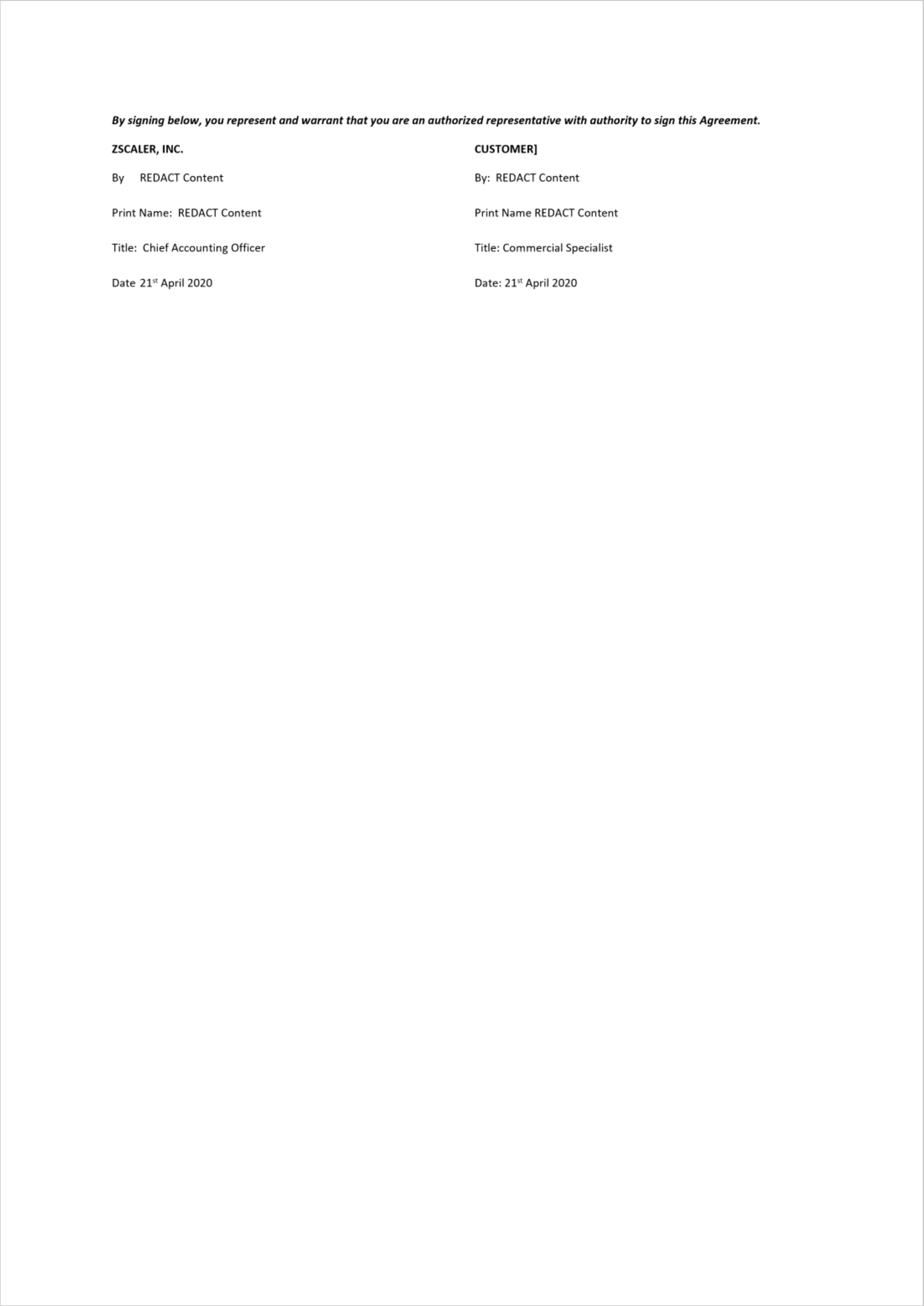
15.12.6. - REDACTED Content

15.13 Publicity and branding. Zscaler shall not: (a) make any press announcements or publicise this Agreement or any Order or its contents in any way; or (b) use the Customer's name or brand in any promotion or marketing or announcement of orders, without approval of the Customer. Notwithstanding the foregoing, Zscaler shall be permitted to include Customer's name in any sales related materials confirming Zscaler's current customer base, provided that such materials shall not be distributed other than to existing and potential future Zscaler customers.

15.14 Variation. No variation to this Agreement (including this Section 15.14) shall be effective unless made in accordance with Section 13 (Change Control Procedure) (or otherwise agreed in writing) and signed by a duly authorised officer of each of the Customer and Zscaler.

Page 10

30 June 2020 14:51

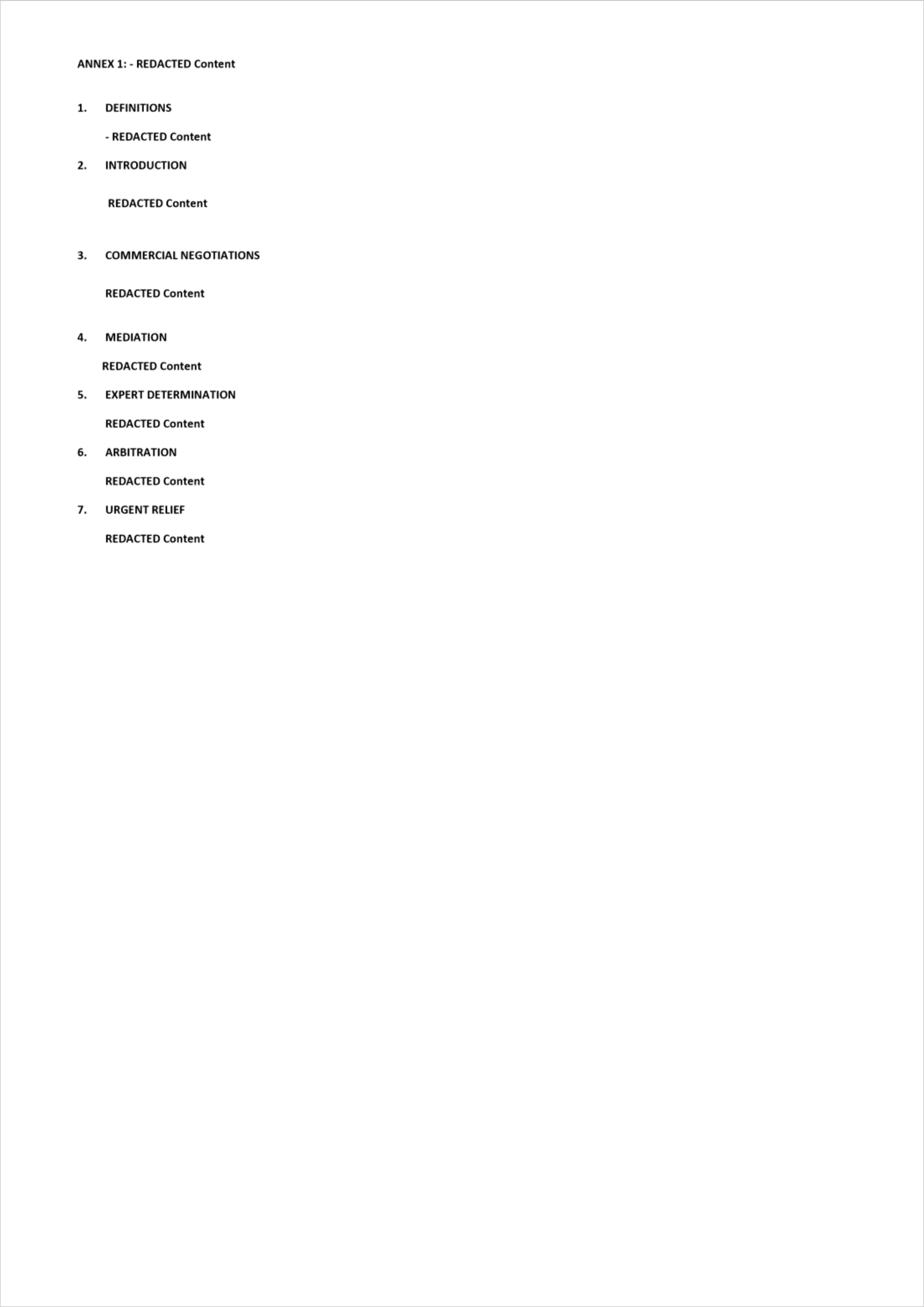


By signing below, you represent and warrant that you are an authorized representative with authority to sign this Agreement.

ZSCALER, INC.	**CUSTOMER]**
By REDACT Content	By: REDACT Content
Print Name: REDACT Content	Print Name REDACT Content
Title: Chief Accounting Officer	Title: Commercial Specialist
Date 21st April 2020	Date: 21st April 2020

Page 11

30 June 2020 14:51



ANNEX 1: - REDACTED Content

1. DEFINITIONS

- REDACTED Content

2. INTRODUCTION

REDACTED Content

3. COMMERCIAL NEGOTIATIONS

REDACTED Content

4. MEDIATION

REDACTED Content

5. EXPERT DETERMINATION

REDACTED Content

6. ARBITRATION

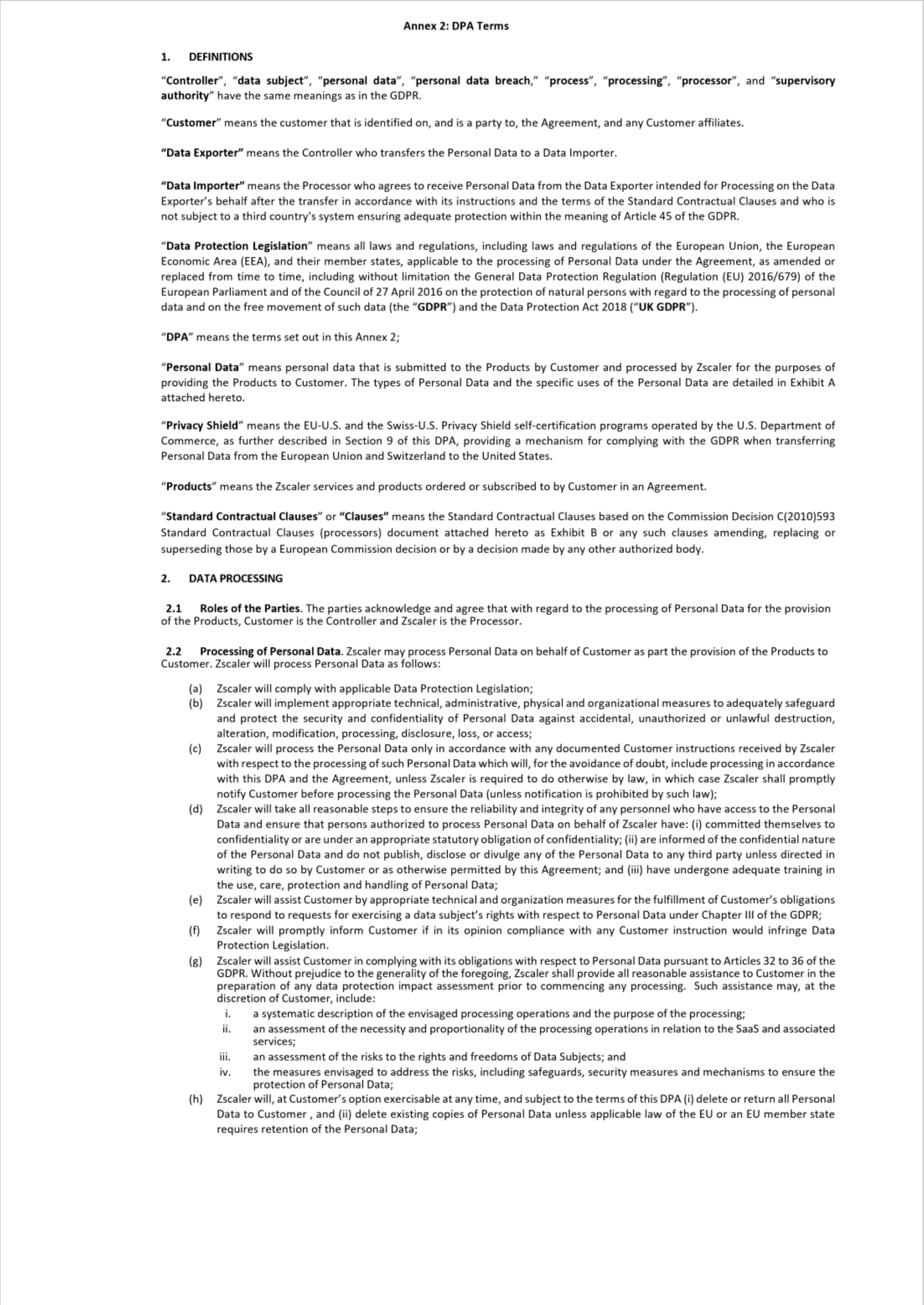
REDACTED Content

7. URGENT RELIEF

REDACTED Content

Page 12

30 June 2020 14:51



Annex 2: DPA Terms

1. DEFINITIONS

"**Controller**", "**data subject**", "**personal data**", "**personal data breach**," "**process**", "**processing**", "**processor**", and "**supervisory authority**" have the same meanings as in the GDPR.

"**Customer**" means the customer that is identified on, and is a party to, the Agreement, and any Customer affiliates.

"Data Exporter" means the Controller who transfers the Personal Data to a Data Importer.

"Data Importer" means the Processor who agrees to receive Personal Data from the Data Exporter intended for Processing on the Data Exporter's behalf after the transfer in accordance with its instructions and the terms of the Standard Contractual Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 45 of the GDPR.

"**Data Protection Legislation**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area (EEA), and their member states, applicable to the processing of Personal Data under the Agreement, as amended or replaced from time to time, including without limitation the General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**") and the Data Protection Act 2018 ("**UK GDPR**").

"**DPA**" means the terms set out in this Annex 2;

"**Personal Data**" means personal data that is submitted to the Products by Customer and processed by Zscaler for the purposes of providing the Products to Customer. The types of Personal Data and the specific uses of the Personal Data are detailed in Exhibit A attached hereto.

"**Privacy Shield**" means the EU-U.S. and the Swiss-U.S. Privacy Shield self-certification programs operated by the U.S. Department of Commerce, as further described in Section 9 of this DPA, providing a mechanism for complying with the GDPR when transferring Personal Data from the European Union and Switzerland to the United States.

"**Products**" means the Zscaler services and products ordered or subscribed to by Customer in an Agreement.

"**Standard Contractual Clauses**" or **"Clauses"** means the Standard Contractual Clauses based on the Commission Decision C(2010)593 Standard Contractual Clauses (processors) document attached hereto as Exhibit B or any such clauses amending, replacing or superseding those by a European Commission decision or by a decision made by any other authorized body.

2. DATA PROCESSING

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Personal Data for the provision of the Products, Customer is the Controller and Zscaler is the Processor.

2.2 Processing of Personal Data. Zscaler may process Personal Data on behalf of Customer as part the provision of the Products to Customer. Zscaler will process Personal Data as follows:

(a) Zscaler will comply with applicable Data Protection Legislation;

(b) Zscaler will implement appropriate technical, administrative, physical and organizational measures to adequately safeguard and protect the security and confidentiality of Personal Data against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access;

(c) Zscaler will process the Personal Data only in accordance with any documented Customer instructions received by Zscaler with respect to the processing of such Personal Data which will, for the avoidance of doubt, include processing in accordance with this DPA and the Agreement, unless Zscaler is required to do otherwise by law, in which case Zscaler shall promptly notify Customer before processing the Personal Data (unless notification is prohibited by such law);

(d) Zscaler will take all reasonable steps to ensure the reliability and integrity of any personnel who have access to the Personal Data and ensure that persons authorized to process Personal Data on behalf of Zscaler have: (i) committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (ii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by Customer or as otherwise permitted by this Agreement; and (iii) have undergone adequate training in the use, care, protection and handling of Personal Data;

(e) Zscaler will assist Customer by appropriate technical and organization measures for the fulfillment of Customer's obligations to respond to requests for exercising a data subject's rights with respect to Personal Data under Chapter III of the GDPR;

(f) Zscaler will promptly inform Customer if in its opinion compliance with any Customer instruction would infringe Data Protection Legislation.

(g) Zscaler will assist Customer in complying with its obligations with respect to Personal Data pursuant to Articles 32 to 36 of the GDPR. Without prejudice to the generality of the foregoing, Zscaler shall provide all reasonable assistance to Customer in the preparation of any data protection impact assessment prior to commencing any processing. Such assistance may, at the discretion of Customer, include:

   i. a systematic description of the envisaged processing operations and the purpose of the processing;

   ii. an assessment of the necessity and proportionality of the processing operations in relation to the SaaS and associated services;

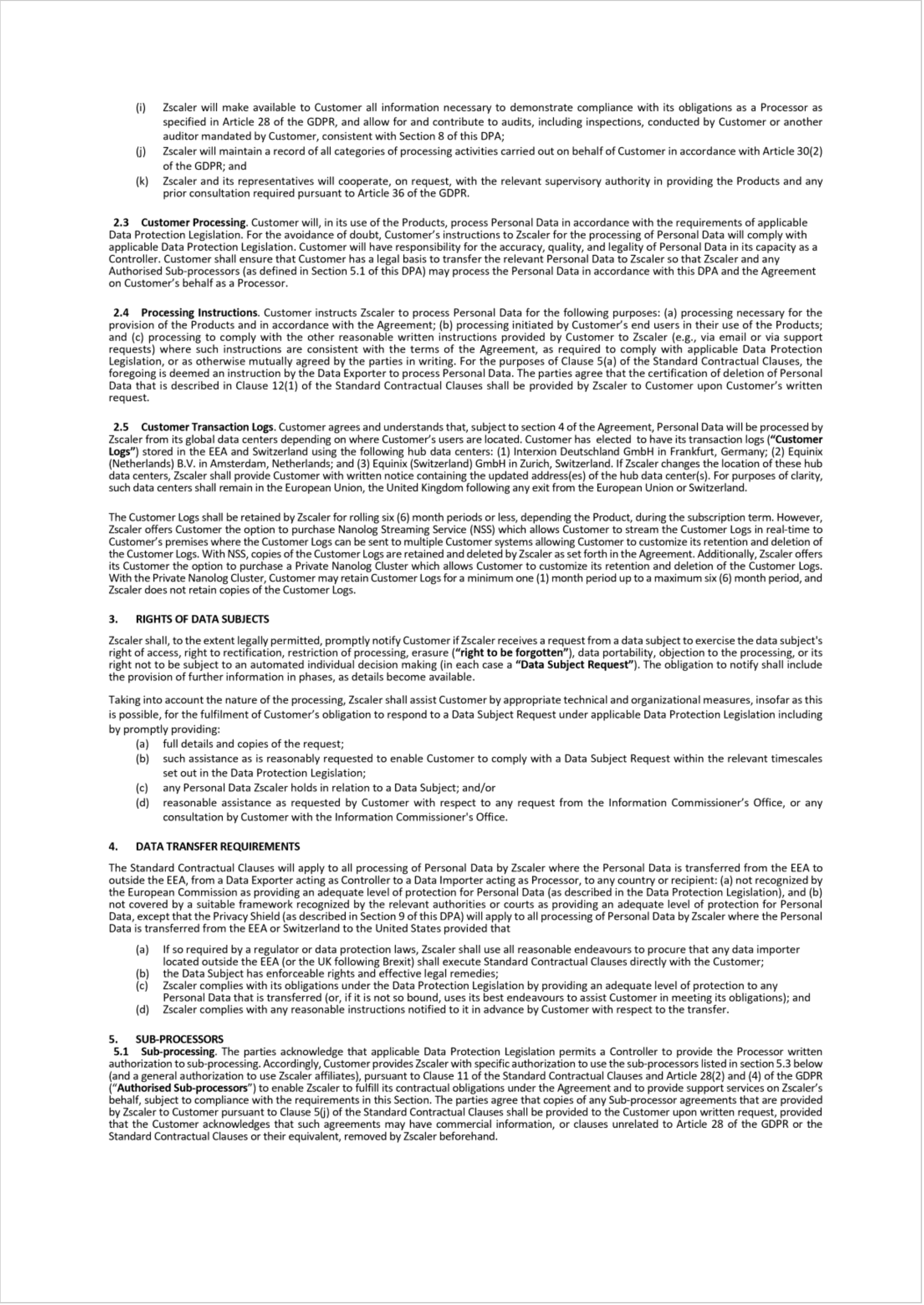
   iii. an assessment of the risks to the rights and freedoms of Data Subjects; and

   iv. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data;

(h) Zscaler will, at Customer's option exercisable at any time, and subject to the terms of this DPA (i) delete or return all Personal Data to Customer , and (ii) delete existing copies of Personal Data unless applicable law of the EU or an EU member state requires retention of the Personal Data;

Page 13

30 June 2020 14:51



(i) Zscaler will make available to Customer all information necessary to demonstrate compliance with its obligations as a Processor as specified in Article 28 of the GDPR, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, consistent with Section 8 of this DPA;

(j) Zscaler will maintain a record of all categories of processing activities carried out on behalf of Customer in accordance with Article 30(2) of the GDPR; and

(k) Zscaler and its representatives will cooperate, on request, with the relevant supervisory authority in providing the Products and any prior consultation required pursuant to Article 36 of the GDPR.

2.3 Customer Processing. Customer will, in its use of the Products, process Personal Data in accordance with the requirements of applicable Data Protection Legislation. For the avoidance of doubt, Customer's instructions to Zscaler for the processing of Personal Data will comply with applicable Data Protection Legislation. Customer will have responsibility for the accuracy, quality, and legality of Personal Data in its capacity as a Controller. Customer shall ensure that Customer has a legal basis to transfer the relevant Personal Data to Zscaler so that Zscaler and any Authorised Sub-processors (as defined in Section 5.1 of this DPA) may process the Personal Data in accordance with this DPA and the Agreement on Customer's behalf as a Processor.

2.4 Processing Instructions. Customer instructs Zscaler to process Personal Data for the following purposes: (a) processing necessary for the provision of the Products and in accordance with the Agreement; (b) processing initiated by Customer's end users in their use of the Products; and (c) processing to comply with the other reasonable written instructions provided by Customer to Zscaler (e.g., via email or via support requests) where such instructions are consistent with the terms of the Agreement, as required to comply with applicable Data Protection Legislation, or as otherwise mutually agreed by the parties in writing. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the foregoing is deemed an instruction by the Data Exporter to process Personal Data. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Zscaler to Customer upon Customer's written request.

2.5 Customer Transaction Logs. Customer agrees and understands that, subject to section 4 of the Agreement, Personal Data will be processed by Zscaler from its global data centers depending on where Customer's users are located. Customer has elected to have its transaction logs (**"Customer Logs"**) stored in the EEA and Switzerland using the following hub data centers: (1) Interxion Deutschland GmbH in Frankfurt, Germany; (2) Equinix (Netherlands) B.V. in Amsterdam, Netherlands; and (3) Equinix (Switzerland) GmbH in Zurich, Switzerland. If Zscaler changes the location of these hub data centers, Zscaler shall provide Customer with written notice containing the updated address(es) of the hub data center(s). For purposes of clarity, such data centers shall remain in the European Union, the United Kingdom following any exit from the European Union or Switzerland.

The Customer Logs shall be retained by Zscaler for rolling six (6) month periods or less, depending the Product, during the subscription term. However, Zscaler offers Customer the option to purchase Nanolog Streaming Service (NSS) which allows Customer to stream the Customer Logs in real-time to Customer's premises where the Customer Logs can be sent to multiple Customer systems allowing Customer to customize its retention and deletion of the Customer Logs. With NSS, copies of the Customer Logs are retained and deleted by Zscaler as set forth in the Agreement. Additionally, Zscaler offers its Customer the option to purchase a Private Nanolog Cluster which allows Customer to customize its retention and deletion of the Customer Logs. With the Private Nanolog Cluster, Customer may retain Customer Logs for a minimum one (1) month period up to a maximum six (6) month period, and Zscaler does not retain copies of the Customer Logs.

3. RIGHTS OF DATA SUBJECTS

Zscaler shall, to the extent legally permitted, promptly notify Customer if Zscaler receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure (**"right to be forgotten"**), data portability, objection to the processing, or its right not to be subject to an automated individual decision making (in each case a **"Data Subject Request"**). The obligation to notify shall include the provision of further information in phases, as details become available.

Taking into account the nature of the processing, Zscaler shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Legislation including by promptly providing:

(a) full details and copies of the request;

(b) such assistance as is reasonably requested to enable Customer to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) any Personal Data Zscaler holds in relation to a Data Subject; and/or

(d) reasonable assistance as requested by Customer with respect to any request from the Information Commissioner's Office, or any consultation by Customer with the Information Commissioner's Office.

4. DATA TRANSFER REQUIREMENTS

The Standard Contractual Clauses will apply to all processing of Personal Data by Zscaler where the Personal Data is transferred from the EEA to outside the EEA, from a Data Exporter acting as Controller to a Data Importer acting as Processor, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Legislation), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, except that the Privacy Shield (as described in Section 9 of this DPA) will apply to all processing of Personal Data by Zscaler where the Personal Data is transferred from the EEA or Switzerland to the United States provided that

(a) If so required by a regulator or data protection laws, Zscaler shall use all reasonable endeavours to procure that any data importer located outside the EEA (or the UK following Brexit) shall execute Standard Contractual Clauses directly with the Customer;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) Zscaler complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist Customer in meeting its obligations); and

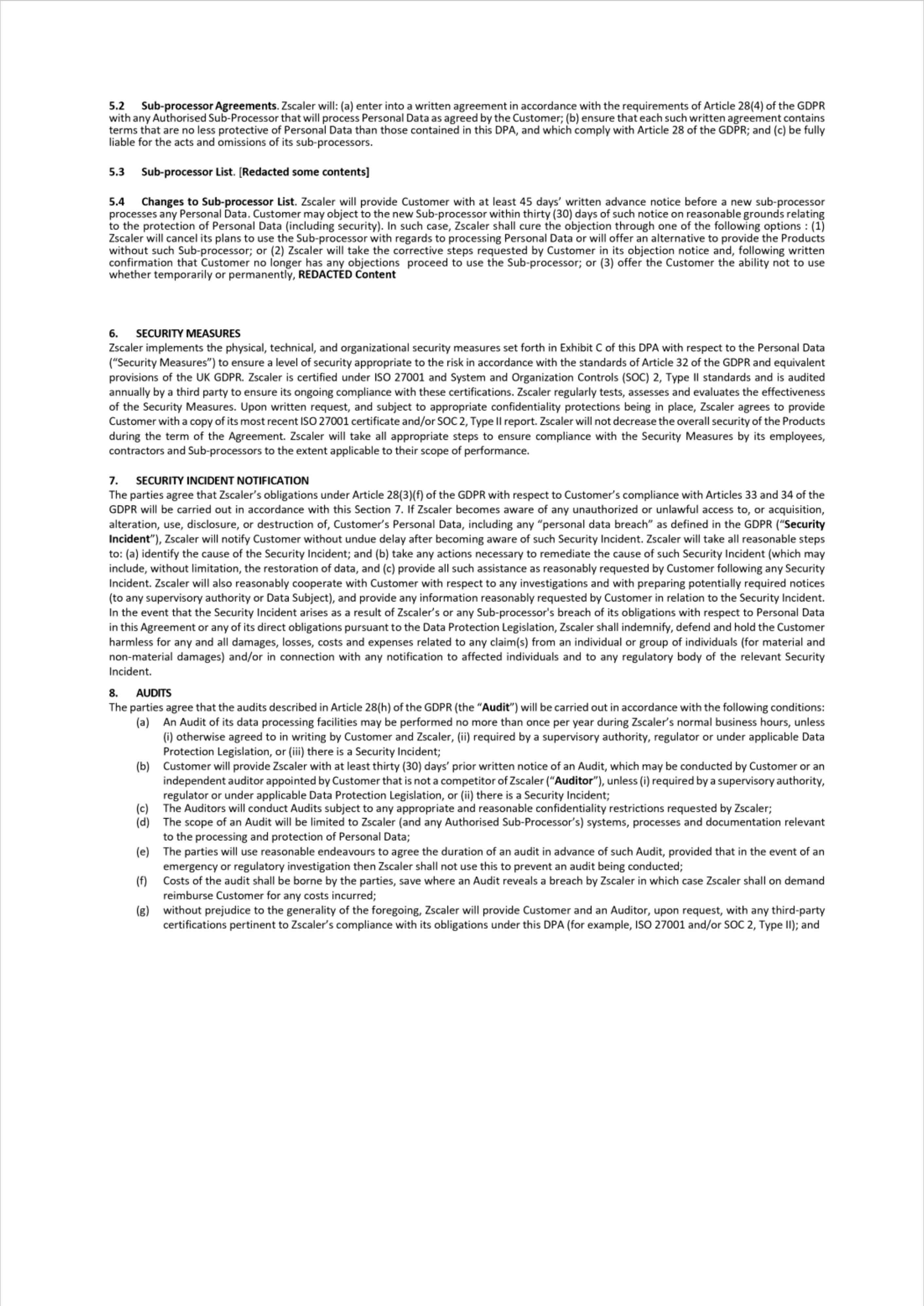
(d) Zscaler complies with any reasonable instructions notified to it in advance by Customer with respect to the transfer.

5. SUB-PROCESSORS

5.1 Sub-processing. The parties acknowledge that applicable Data Protection Legislation permits a Controller to provide the Processor written authorization to sub-processing. Accordingly, Customer provides Zscaler with specific authorization to use the sub-processors listed in section 5.3 below (and a general authorization to use Zscaler affiliates), pursuant to Clause 11 of the Standard Contractual Clauses and Article 28(2) and (4) of the GDPR ("**Authorised Sub-processors**") to enable Zscaler to fulfill its contractual obligations under the Agreement and to provide support services on Zscaler's behalf, subject to compliance with the requirements in this Section. The parties agree that copies of any Sub-processor agreements that are provided by Zscaler to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses shall be provided to the Customer upon written request, provided that the Customer acknowledges that such agreements may have commercial information, or clauses unrelated to Article 28 of the GDPR or the Standard Contractual Clauses or their equivalent, removed by Zscaler beforehand.

Page 14

30 June 2020 14:51



5.2 Sub-processor Agreements. Zscaler will: (a) enter into a written agreement in accordance with the requirements of Article 28(4) of the GDPR with any Authorised Sub-Processor that will process Personal Data as agreed by the Customer; (b) ensure that each such written agreement contains terms that are no less protective of Personal Data than those contained in this DPA, and which comply with Article 28 of the GDPR; and (c) be fully liable for the acts and omissions of its sub-processors.

5.3 Sub-processor List. [**Redacted some contents]**

5.4 Changes to Sub-processor List. Zscaler will provide Customer with at least 45 days' written advance notice before a new sub-processor processes any Personal Data. Customer may object to the new Sub-processor within thirty (30) days of such notice on reasonable grounds relating to the protection of Personal Data (including security). In such case, Zscaler shall cure the objection through one of the following options : (1) Zscaler will cancel its plans to use the Sub-processor with regards to processing Personal Data or will offer an alternative to provide the Products without such Sub-processor; or (2) Zscaler will take the corrective steps requested by Customer in its objection notice and, following written confirmation that Customer no longer has any objections proceed to use the Sub-processor; or (3) offer the Customer the ability not to use whether temporarily or permanently, **REDACTED Content**

6. SECURITY MEASURES

Zscaler implements the physical, technical, and organizational security measures set forth in Exhibit C of this DPA with respect to the Personal Data ("Security Measures") to ensure a level of security appropriate to the risk in accordance with the standards of Article 32 of the GDPR and equivalent provisions of the UK GDPR. Zscaler is certified under ISO 27001 and System and Organization Controls (SOC) 2, Type II standards and is audited annually by a third party to ensure its ongoing compliance with these certifications. Zscaler regularly tests, assesses and evaluates the effectiveness of the Security Measures. Upon written request, and subject to appropriate confidentiality protections being in place, Zscaler agrees to provide Customer with a copy of its most recent ISO 27001 certificate and/or SOC 2, Type II report. Zscaler will not decrease the overall security of the Products during the term of the Agreement. Zscaler will take all appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance.

7. SECURITY INCIDENT NOTIFICATION

The parties agree that Zscaler's obligations under Article 28(3)(f) of the GDPR with respect to Customer's compliance with Articles 33 and 34 of the GDPR will be carried out in accordance with this Section 7. If Zscaler becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer's Personal Data, including any "personal data breach" as defined in the GDPR ("**Security Incident**"), Zscaler will notify Customer without undue delay after becoming aware of such Security Incident. Zscaler will take all reasonable steps to: (a) identify the cause of the Security Incident; and (b) take any actions necessary to remediate the cause of such Security Incident (which may include, without limitation, the restoration of data, and (c) provide all such assistance as reasonably requested by Customer following any Security Incident. Zscaler will also reasonably cooperate with Customer with respect to any investigations and with preparing potentially required notices (to any supervisory authority or Data Subject), and provide any information reasonably requested by Customer in relation to the Security Incident. In the event that the Security Incident arises as a result of Zscaler's or any Sub-processor's breach of its obligations with respect to Personal Data in this Agreement or any of its direct obligations pursuant to the Data Protection Legislation, Zscaler shall indemnify, defend and hold the Customer harmless for any and all damages, losses, costs and expenses related to any claim(s) from an individual or group of individuals (for material and non-material damages) and/or in connection with any notification to affected individuals and to any regulatory body of the relevant Security Incident.

8. AUDITS

The parties agree that the audits described in Article 28(h) of the GDPR (the "**Audit**") will be carried out in accordance with the following conditions:

(a) An Audit of its data processing facilities may be performed no more than once per year during Zscaler's normal business hours, unless (i) otherwise agreed to in writing by Customer and Zscaler, (ii) required by a supervisory authority, regulator or under applicable Data Protection Legislation, or (iii) there is a Security Incident;

(b) Customer will provide Zscaler with at least thirty (30) days' prior written notice of an Audit, which may be conducted by Customer or an independent auditor appointed by Customer that is not a competitor of Zscaler ("**Auditor**"), unless (i) required by a supervisory authority, regulator or under applicable Data Protection Legislation, or (ii) there is a Security Incident;

(c) The Auditors will conduct Audits subject to any appropriate and reasonable confidentiality restrictions requested by Zscaler;

(d) The scope of an Audit will be limited to Zscaler (and any Authorised Sub-Processor's) systems, processes and documentation relevant to the processing and protection of Personal Data;

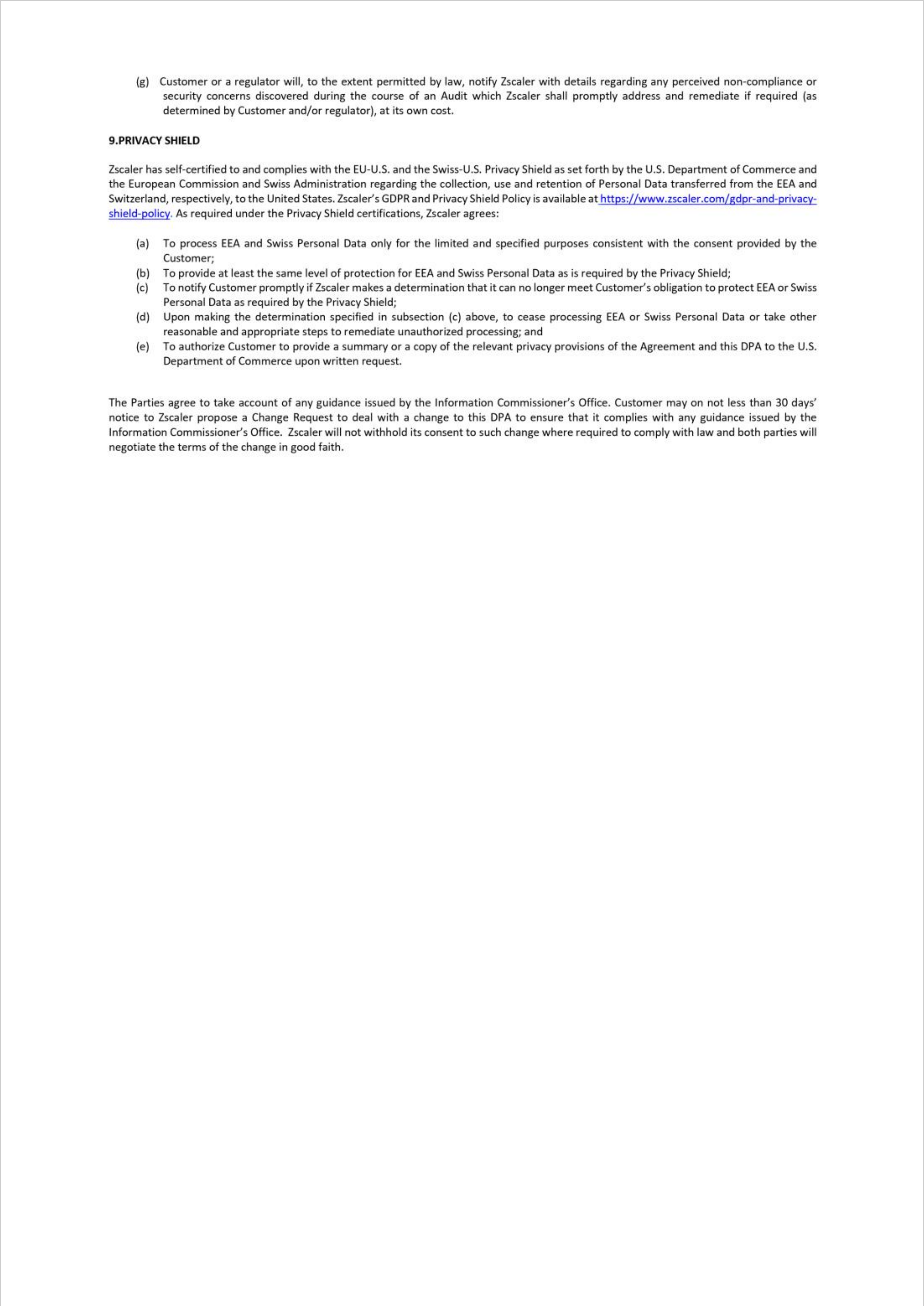
(e) The parties will use reasonable endeavours to agree the duration of an audit in advance of such Audit, provided that in the event of an emergency or regulatory investigation then Zscaler shall not use this to prevent an audit being conducted;

(f) Costs of the audit shall be borne by the parties, save where an Audit reveals a breach by Zscaler in which case Zscaler shall on demand reimburse Customer for any costs incurred;

(g) without prejudice to the generality of the foregoing, Zscaler will provide Customer and an Auditor, upon request, with any third-party certifications pertinent to Zscaler's compliance with its obligations under this DPA (for example, ISO 27001 and/or SOC 2, Type II); and

Page 15

30 June 2020 14:51



(g) Customer or a regulator will, to the extent permitted by law, notify Zscaler with details regarding any perceived non-compliance or security concerns discovered during the course of an Audit which Zscaler shall promptly address and remediate if required (as determined by Customer and/or regulator), at its own cost.

9.PRIVACY SHIELD

Zscaler has self-certified to and complies with the EU-U.S. and the Swiss-U.S. Privacy Shield as set forth by the U.S. Department of Commerce and the European Commission and Swiss Administration regarding the collection, use and retention of Personal Data transferred from the EEA and Switzerland, respectively, to the United States. Zscaler's GDPR and Privacy Shield Policy is available at https://www.zscaler.com/gdpr-and-privacy-shield-policy. As required under the Privacy Shield certifications, Zscaler agrees:

(a) To process EEA and Swiss Personal Data only for the limited and specified purposes consistent with the consent provided by the Customer;
(b) To provide at least the same level of protection for EEA and Swiss Personal Data as is required by the Privacy Shield;
(c) To notify Customer promptly if Zscaler makes a determination that it can no longer meet Customer's obligation to protect EEA or Swiss Personal Data as required by the Privacy Shield;
(d) Upon making the determination specified in subsection (c) above, to cease processing EEA or Swiss Personal Data or take other reasonable and appropriate steps to remediate unauthorized processing; and
(e) To authorize Customer to provide a summary or a copy of the relevant privacy provisions of the Agreement and this DPA to the U.S. Department of Commerce upon written request.

The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Customer may on not less than 30 days' notice to Zscaler propose a Change Request to deal with a change to this DPA to ensure that it complies with any guidance issued by the Information Commissioner's Office. Zscaler will not withhold its consent to such change where required to comply with law and both parties will negotiate the terms of the change in good faith.

Page 16

30 June 2020 14:51

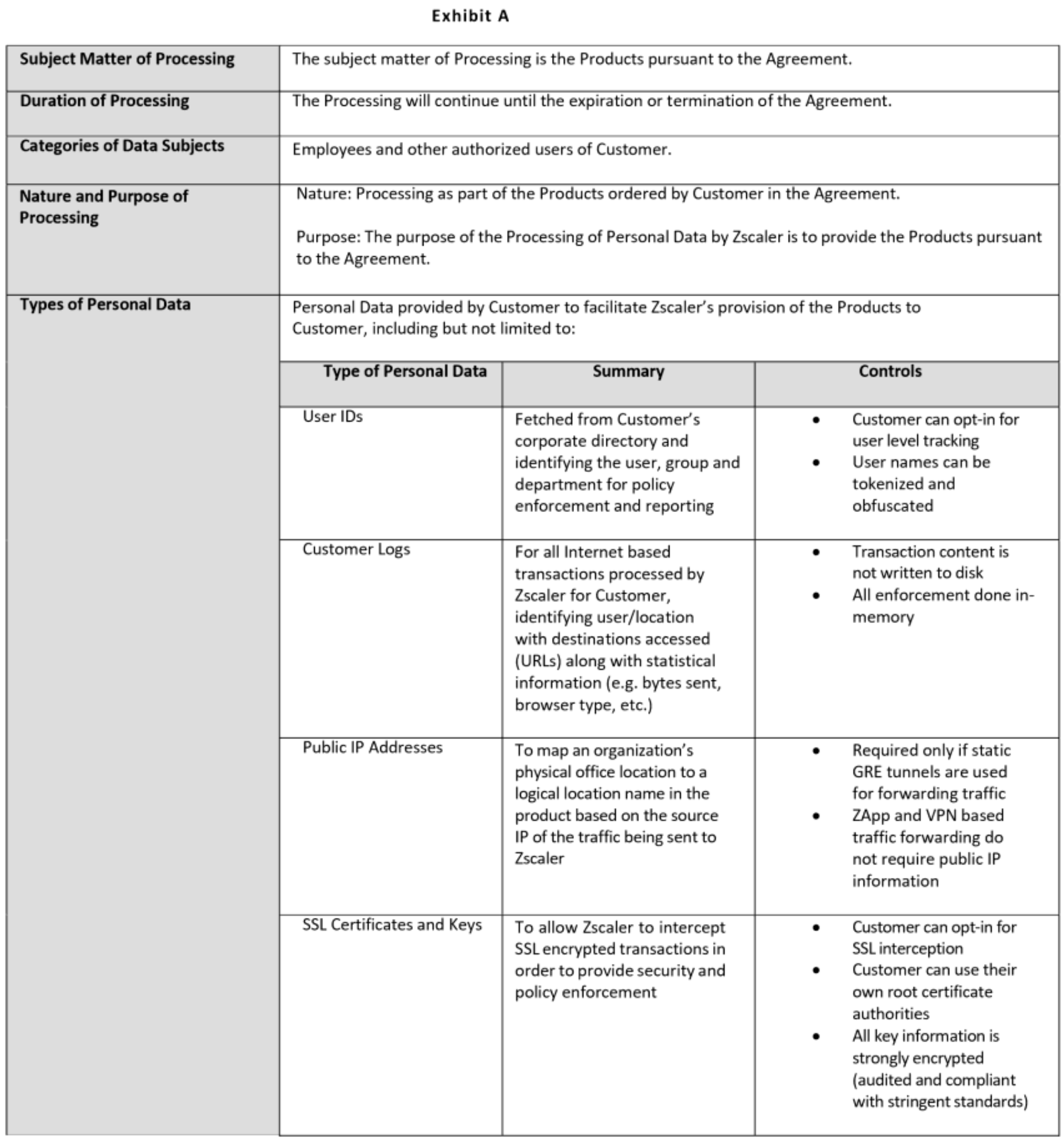


Exhibit A

Subject Matter of Processing	The subject matter of Processing is the Products pursuant to the Agreement.
Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
Categories of Data Subjects	Employees and other authorized users of Customer.
Nature and Purpose of Processing	Nature: Processing as part of the Products ordered by Customer in the Agreement. Purpose: The purpose of the Processing of Personal Data by Zscaler is to provide the Products pursuant to the Agreement.
Types of Personal Data	Personal Data provided by Customer to facilitate Zscaler's provision of the Products to Customer, including but not limited to:

Type of Personal Data	**Summary**	**Controls**
User IDs	Fetched from Customer's corporate directory and identifying the user, group and department for policy enforcement and reporting	• Customer can opt-in for user level tracking • User names can be tokenized and obfuscated
Customer Logs	For all Internet based transactions processed by Zscaler for Customer, identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.)	• Transaction content is not written to disk • All enforcement done in-memory
Public IP Addresses	To map an organization's physical office location to a logical location name in the product based on the source IP of the traffic being sent to Zscaler	• Required only if static GRE tunnels are used for forwarding traffic • ZApp and VPN based traffic forwarding do not require public IP information
SSL Certificates and Keys	To allow Zscaler to intercept SSL encrypted transactions in order to provide security and policy enforcement	• Customer can opt-in for SSL interception • Customer can use their own root certificate authorities • All key information is strongly encrypted (audited and compliant with stringent standards)

Page 17

30 June 2020 14:51

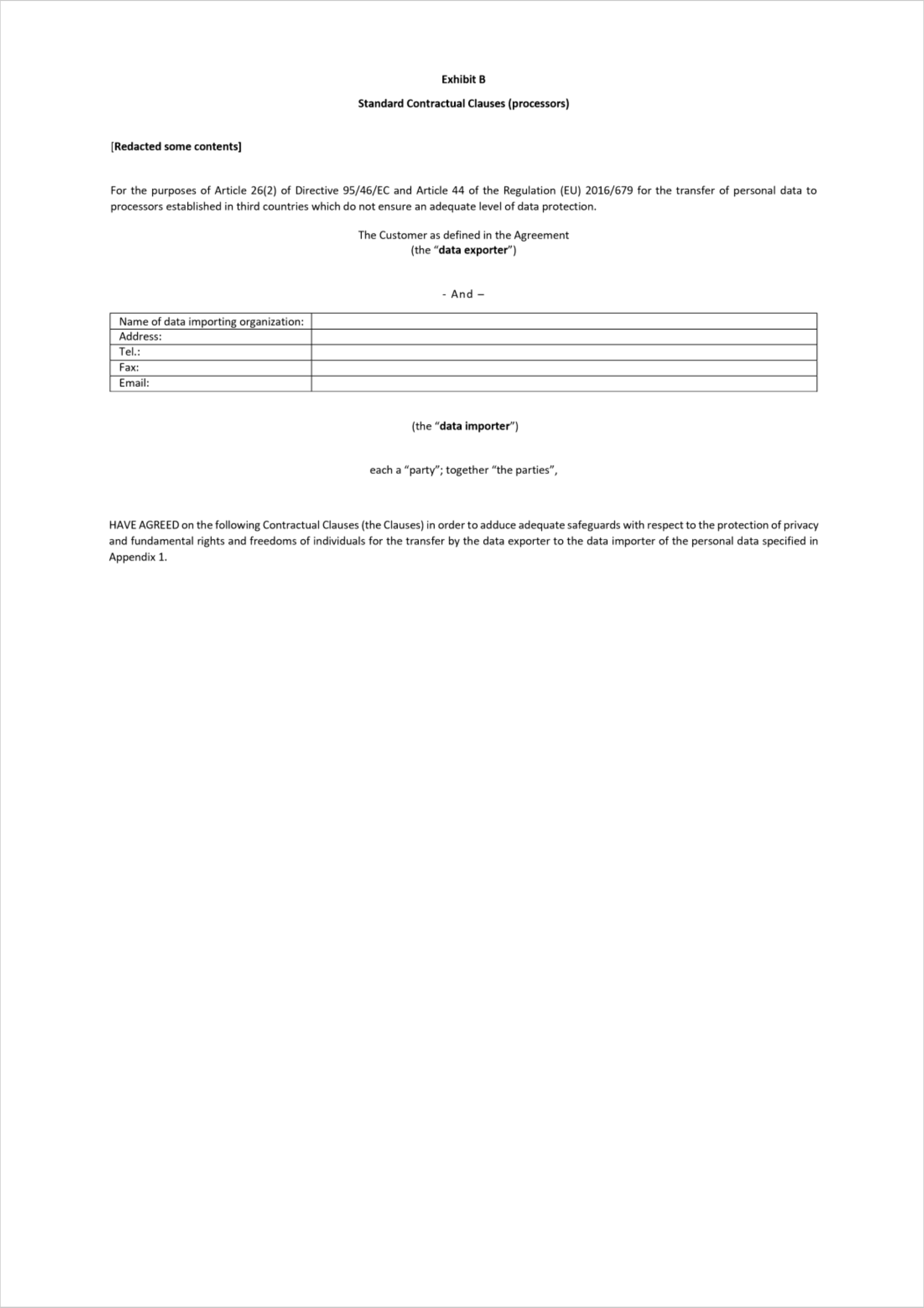


Exhibit B

Standard Contractual Clauses (processors)

[**Redacted some contents]**

For the purposes of Article 26(2) of Directive 95/46/EC and Article 44 of the Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The Customer as defined in the Agreement
(the "**data exporter**")

- And –

Name of data importing organization:	
Address:	
Tel.:	
Fax:	
Email:	

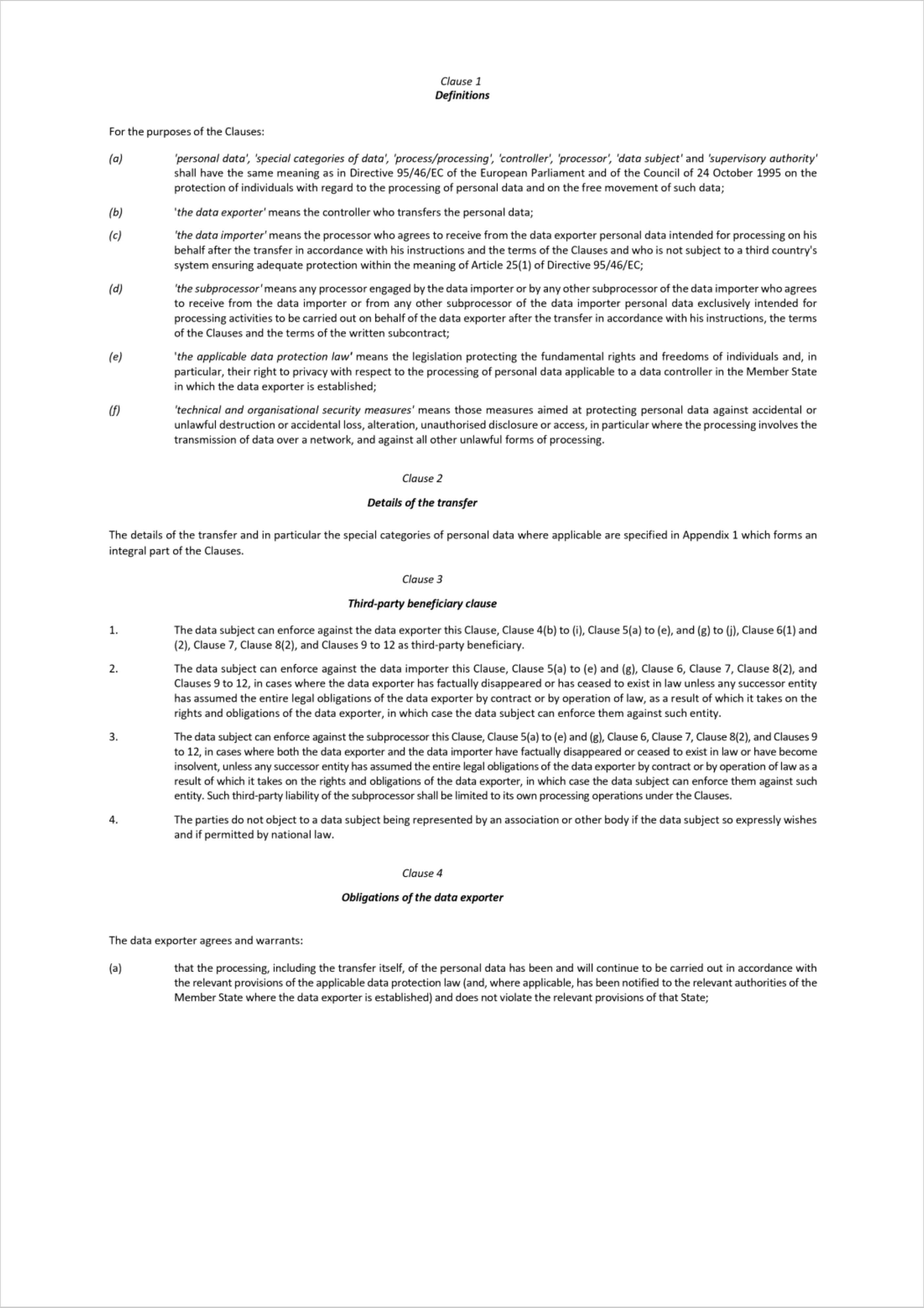
(the "**data importer**")

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.

Page 18

30 June 2020 14:51



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;

(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.

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;

Page 19

30 June 2020 14:51

(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

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;

(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

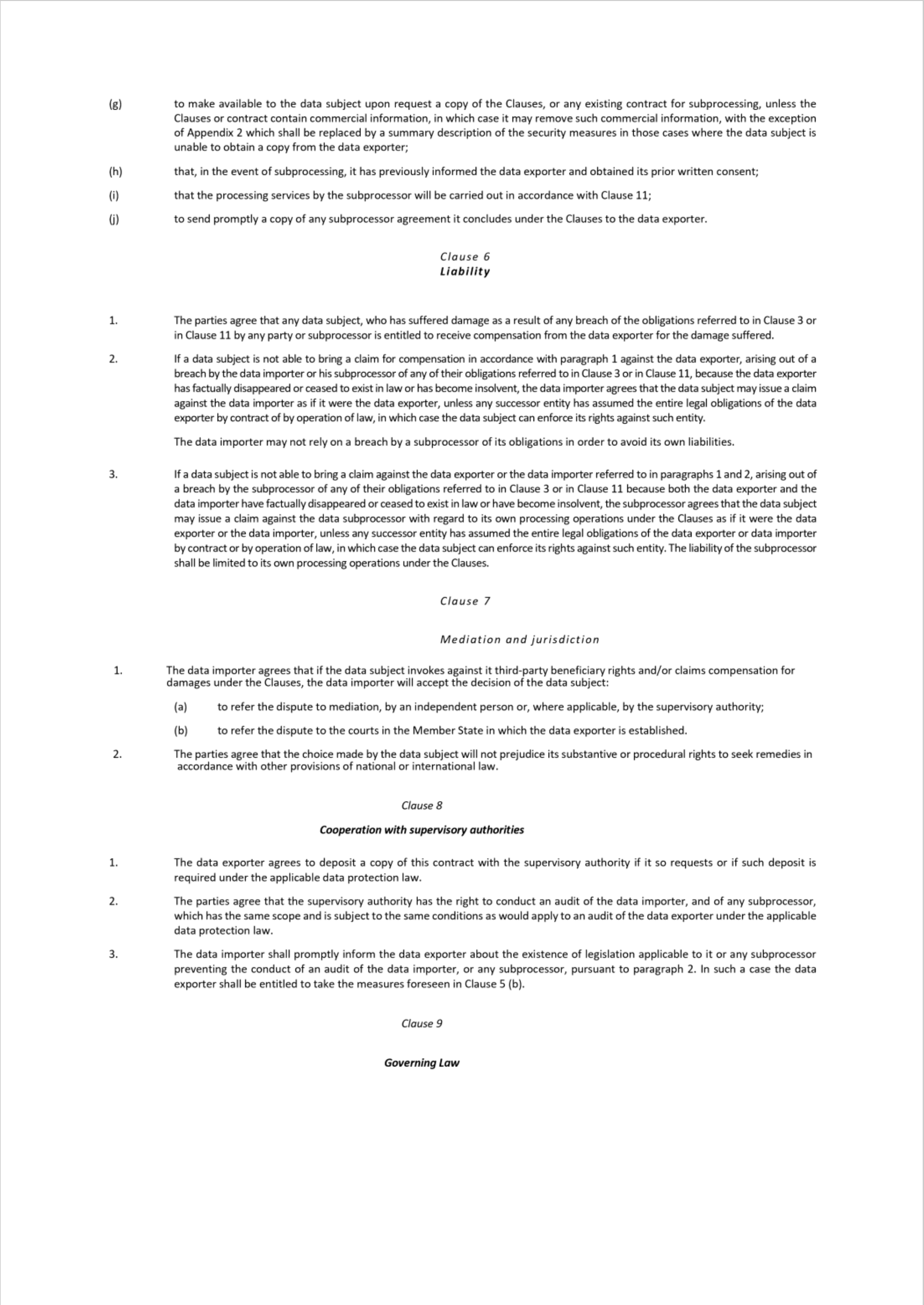
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(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;

Page 20

30 June 2020 14:51



(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.

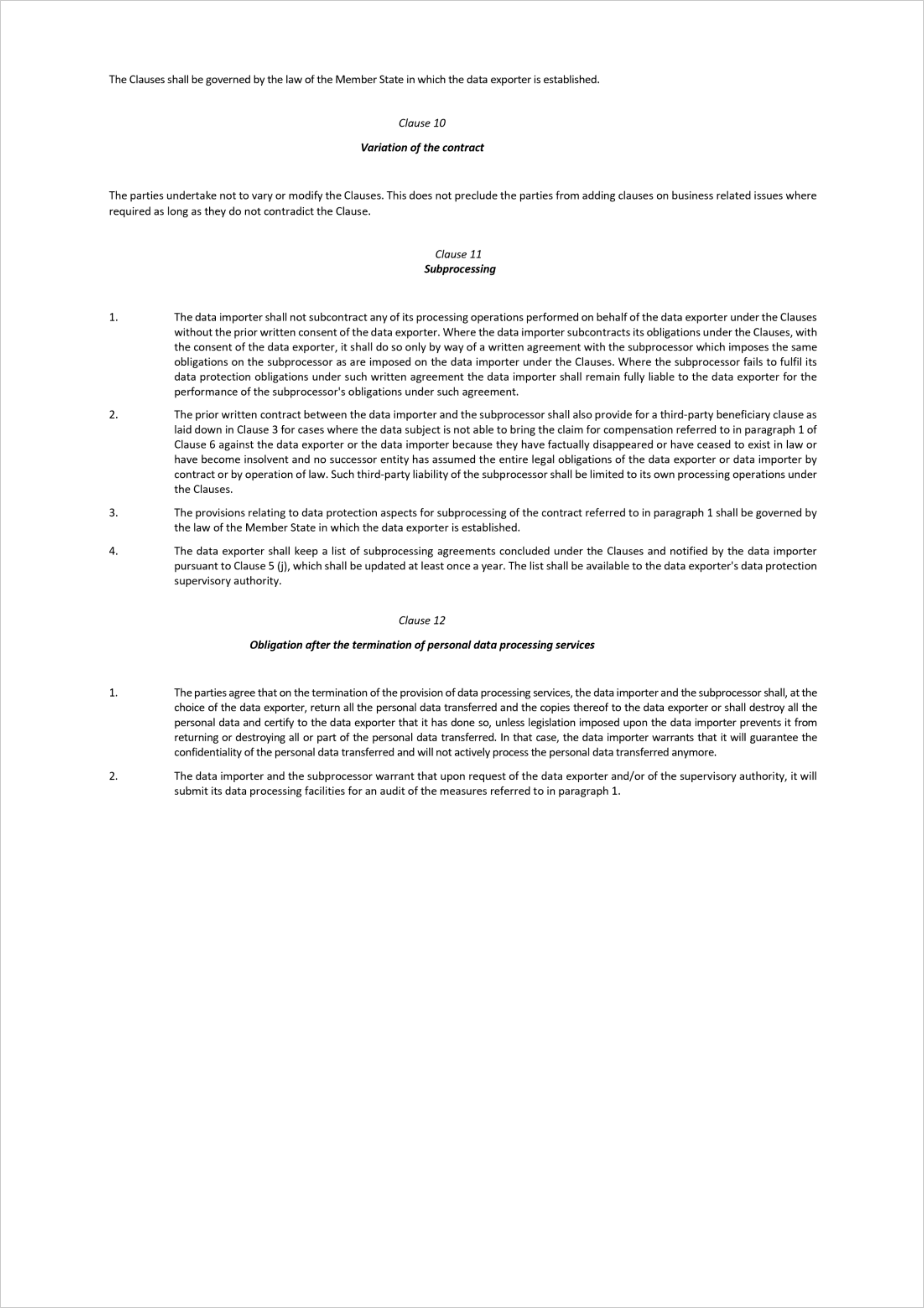
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures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

Clause 9

Governing Law

Page 21

30 June 2020 14:51



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. 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.

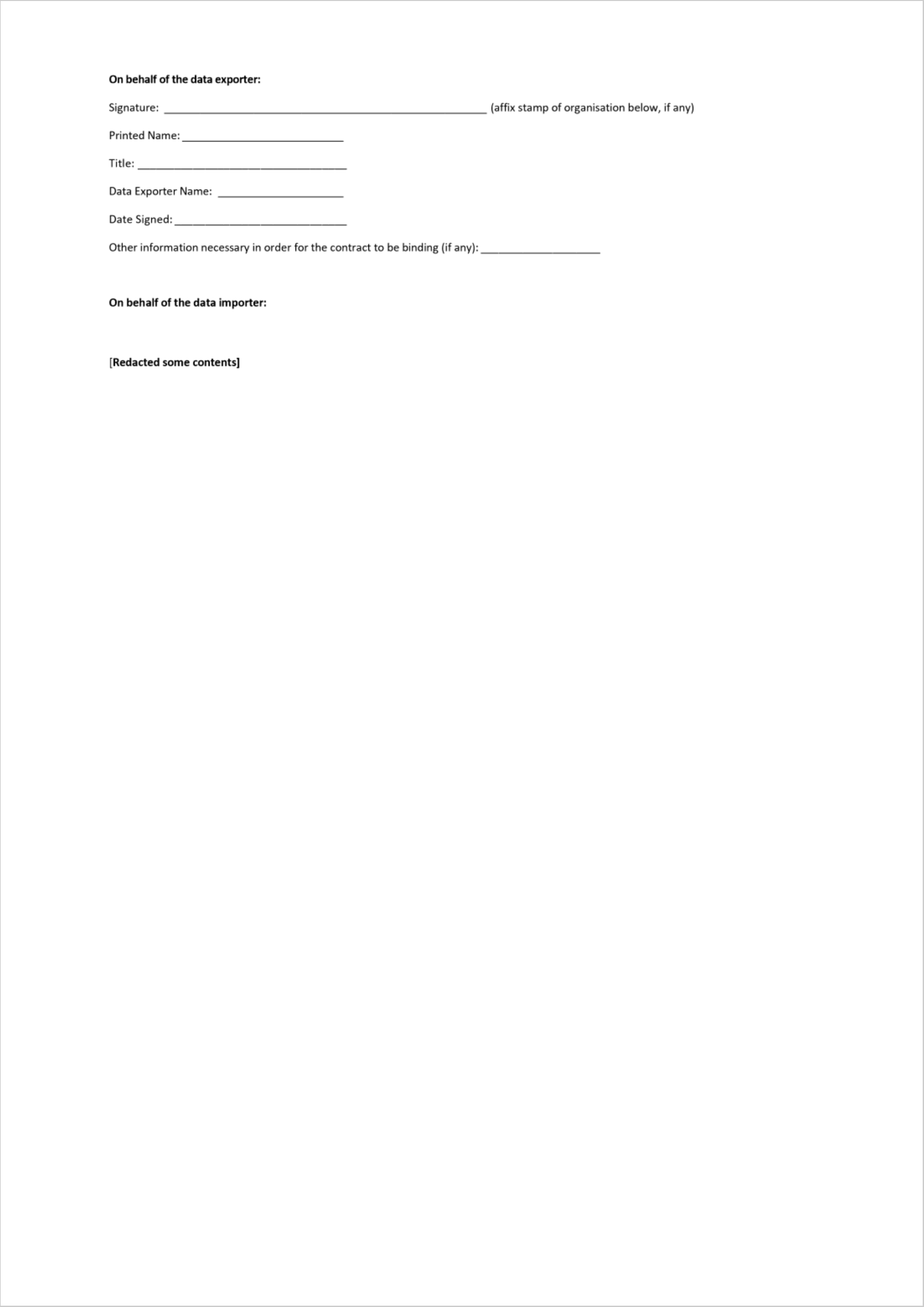
Clause 12

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.

Page 22

30 June 2020 14:51



On behalf of the data exporter:

Signature: ____ (affix stamp of organisation below, if any)

Printed Name: _______________________

Title: ______________________________

Data Exporter Name: __________________

Date Signed: _________________________

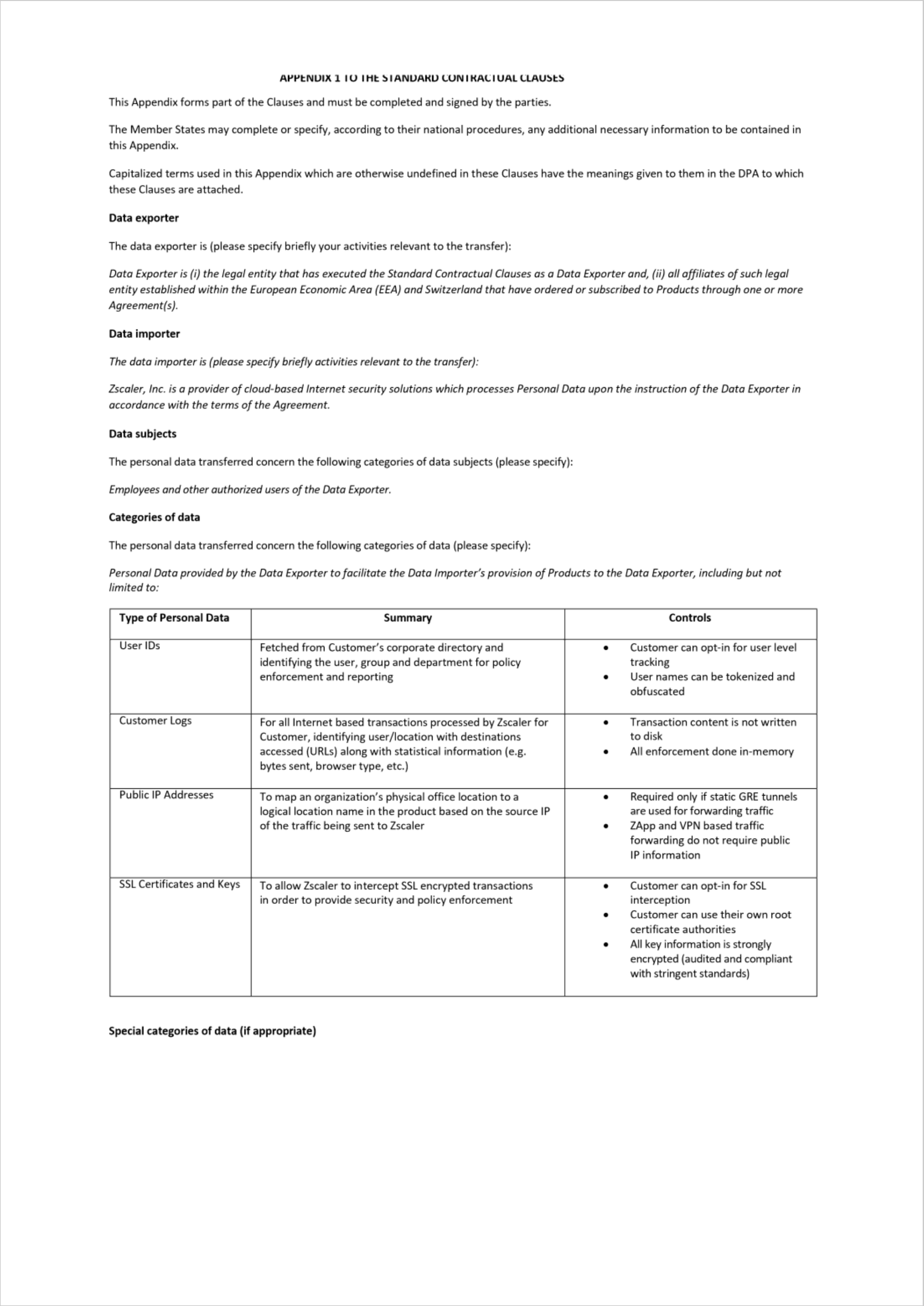
Other information necessary in order for the contract to be binding (if any): _________________

On behalf of the data importer:

[**Redacted some contents]**

Page 23

30 June 2020 14:51



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.

Capitalized terms used in this Appendix which are otherwise undefined in these Clauses have the meanings given to them in the DPA to which these Clauses are attached.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all affiliates of such legal entity established within the European Economic Area (EEA) and Switzerland that have ordered or subscribed to Products through one or more Agreement(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Zscaler, Inc. is a provider of cloud-based Internet security solutions which processes Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees and other authorized users of the Data Exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

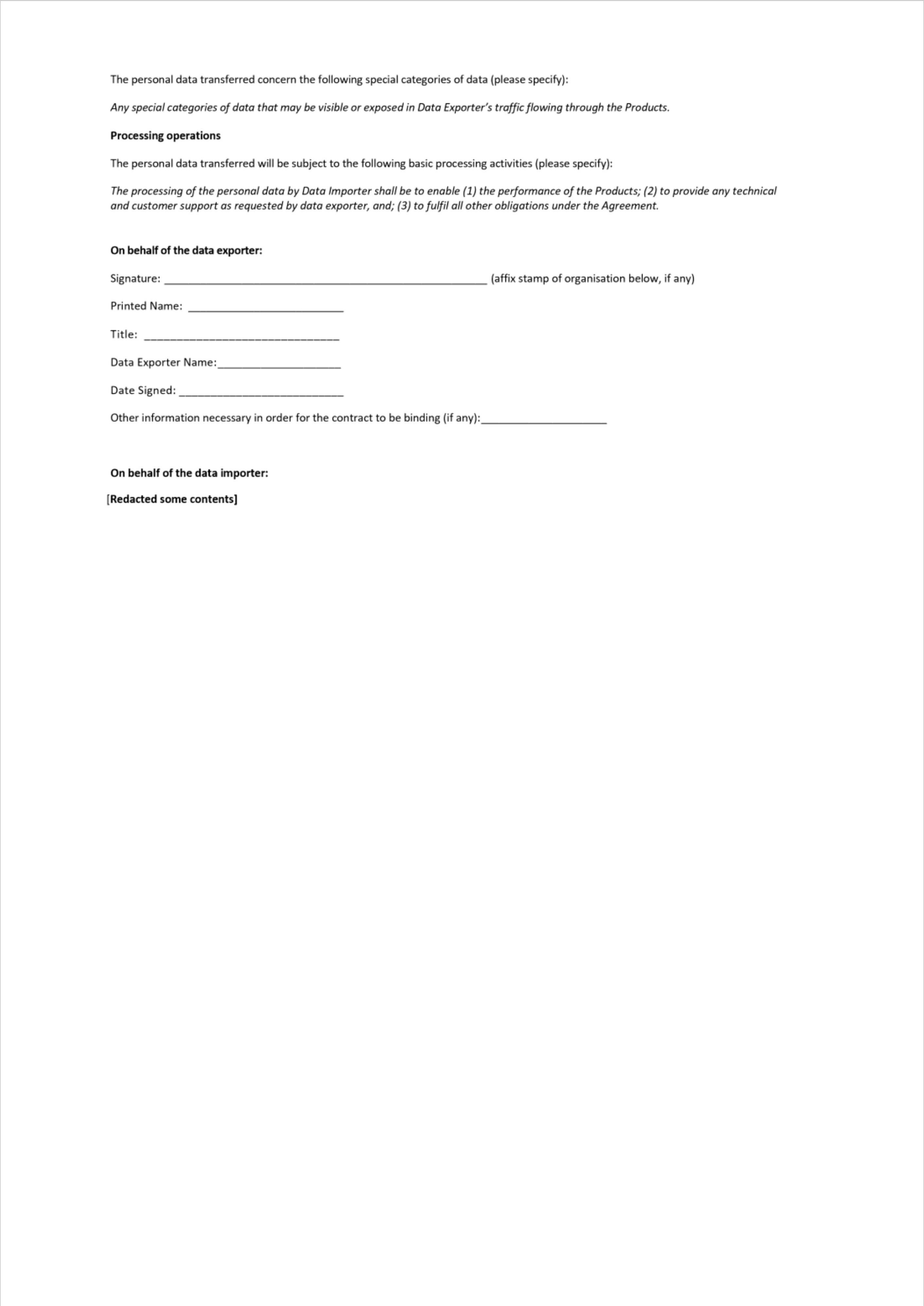
Personal Data provided by the Data Exporter to facilitate the Data Importer's provision of Products to the Data Exporter, including but not limited to:

Type of Personal Data	Summary	Controls
User IDs	Fetched from Customer's corporate directory and identifying the user, group and department for policy enforcement and reporting	• Customer can opt-in for user level tracking • User names can be tokenized and obfuscated
Customer Logs	For all Internet based transactions processed by Zscaler for Customer, identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.)	• Transaction content is not written to disk • All enforcement done in-memory
Public IP Addresses	To map an organization's physical office location to a logical location name in the product based on the source IP of the traffic being sent to Zscaler	• Required only if static GRE tunnels are used for forwarding traffic • ZApp and VPN based traffic forwarding do not require public IP information
SSL Certificates and Keys	To allow Zscaler to intercept SSL encrypted transactions in order to provide security and policy enforcement	• Customer can opt-in for SSL interception • Customer can use their own root certificate authorities • All key information is strongly encrypted (audited and compliant with stringent standards)

Special categories of data (if appropriate)

Page 24

30 June 2020 14:51



The personal data transferred concern the following special categories of data (please specify):

Any special categories of data that may be visible or exposed in Data Exporter's traffic flowing through the Products.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing of the personal data by Data Importer shall be to enable (1) the performance of the Products; (2) to provide any technical and customer support as requested by data exporter, and; (3) to fulfil all other obligations under the Agreement.

On behalf of the data exporter:

Signature: ______________________________ (affix stamp of organisation below, if any)

Printed Name: ______________________

Title: ______________________________

Data Exporter Name:__________________

Date Signed: ________________________

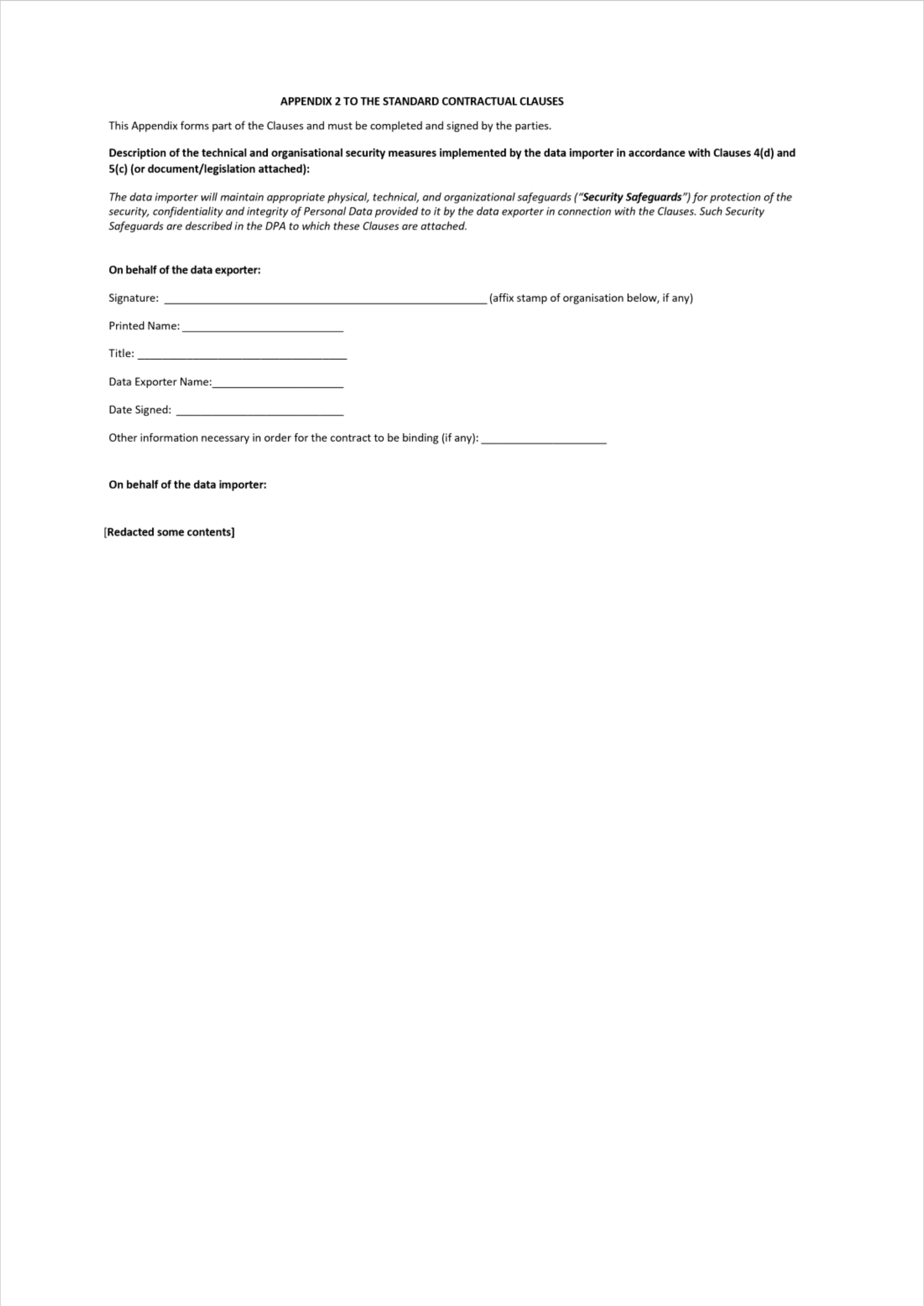
Other information necessary in order for the contract to be binding (if any):____________________

On behalf of the data importer:

[**Redacted some contents]**

Page 25

30 June 2020 14:51



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):

*The data importer will maintain appropriate physical, technical, and organizational safeguards ("****Security Safeguards****") for protection of the security, confidentiality and integrity of Personal Data provided to it by the data exporter in connection with the Clauses. Such Security Safeguards are described in the DPA to which these Clauses are attached.*

On behalf of the data exporter:

Signature: ____ (affix stamp of organisation below, if any)

Printed Name: ______________________

Title: _____________________________

Data Exporter Name:__________________

Date Signed: _______________________

Other information necessary in order for the contract to be binding (if any): _________________

On behalf of the data importer:

[**Redacted some contents]**

Page 26

30 June 2020 14:51

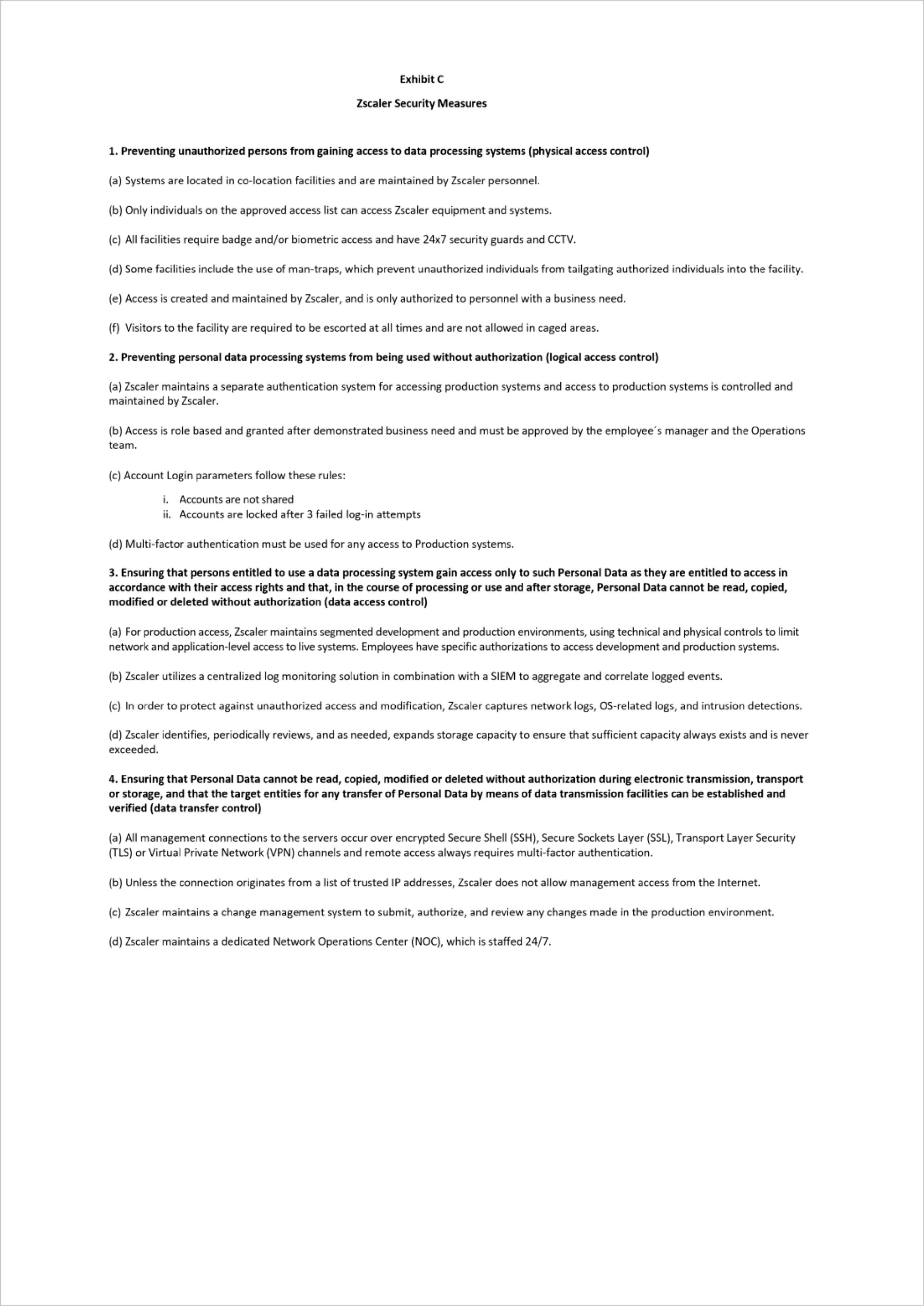


Exhibit C

Zscaler Security Measures

1. Preventing unauthorized persons from gaining access to data processing systems (physical access control)

(a) Systems are located in co-location facilities and are maintained by Zscaler personnel.

(b) Only individuals on the approved access list can access Zscaler equipment and systems.

(c) All facilities require badge and/or biometric access and have 24x7 security guards and CCTV.

(d) Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

(e) Access is created and maintained by Zscaler, and is only authorized to personnel with a business need.

(f) Visitors to the facility are required to be escorted at all times and are not allowed in caged areas.

2. Preventing personal data processing systems from being used without authorization (logical access control)

(a) Zscaler maintains a separate authentication system for accessing production systems and access to production systems is controlled and maintained by Zscaler.

(b) Access is role based and granted after demonstrated business need and must be approved by the employee´s manager and the Operations team.

(c) Account Login parameters follow these rules:

i. Accounts are not shared
ii. Accounts are locked after 3 failed log-in attempts

(d) Multi-factor authentication must be used for any access to Production systems.

3. Ensuring that persons entitled to use a data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control)

(a) For production access, Zscaler maintains segmented development and production environments, using technical and physical controls to limit network and application-level access to live systems. Employees have specific authorizations to access development and production systems.

(b) Zscaler utilizes a centralized log monitoring solution in combination with a SIEM to aggregate and correlate logged events.

(c) In order to protect against unauthorized access and modification, Zscaler captures network logs, OS-related logs, and intrusion detections.

(d) Zscaler identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never exceeded.

4. Ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control)

(a) All management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), Transport Layer Security (TLS) or Virtual Private Network (VPN) channels and remote access always requires multi-factor authentication.

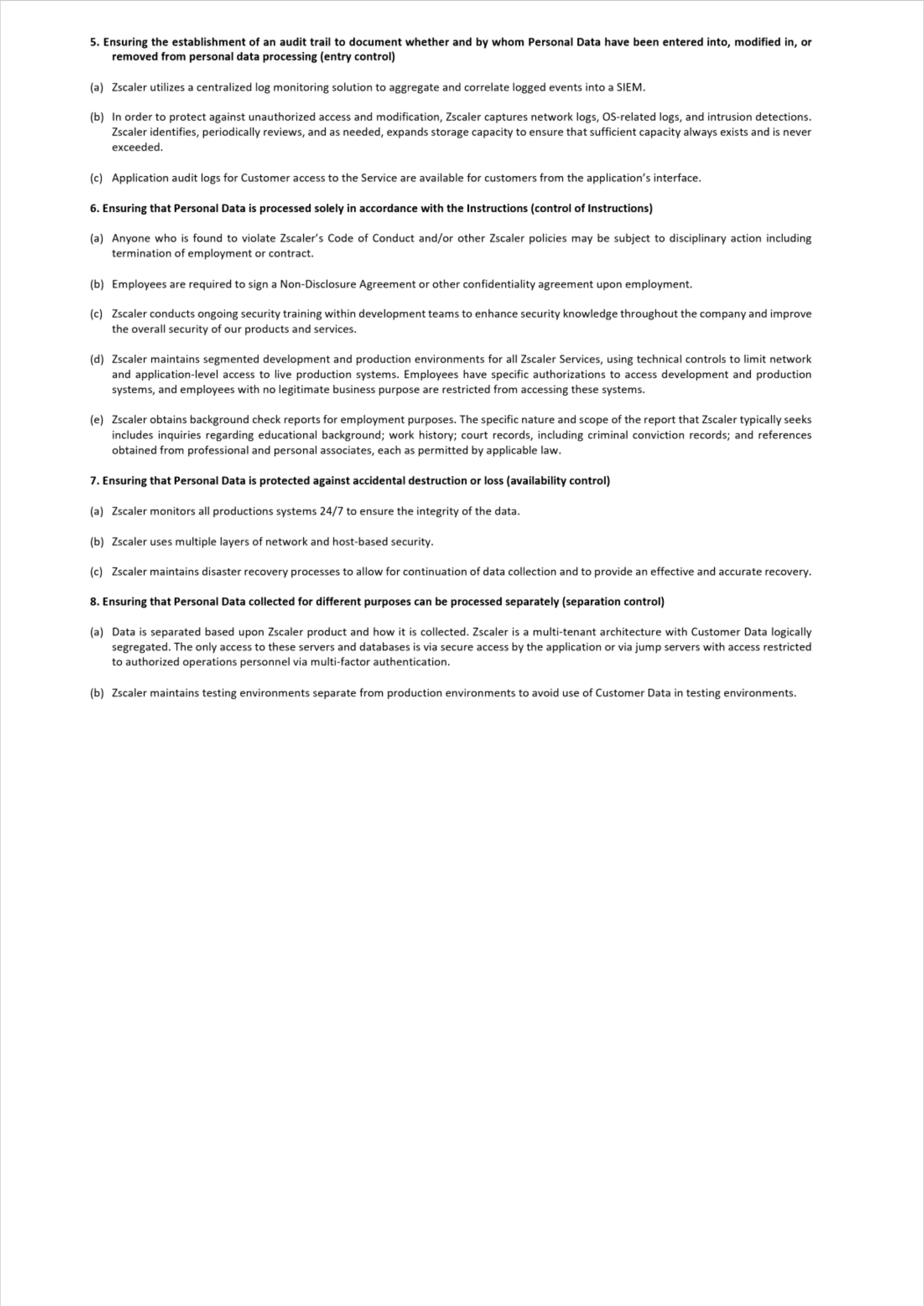
(b) Unless the connection originates from a list of trusted IP addresses, Zscaler does not allow management access from the Internet.

(c) Zscaler maintains a change management system to submit, authorize, and review any changes made in the production environment.

(d) Zscaler maintains a dedicated Network Operations Center (NOC), which is staffed 24/7.

Page 27

30 June 2020 14:51



5. Ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from personal data processing (entry control)

(a) Zscaler utilizes a centralized log monitoring solution to aggregate and correlate logged events into a SIEM.

(b) In order to protect against unauthorized access and modification, Zscaler captures network logs, OS-related logs, and intrusion detections. Zscaler identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never exceeded.

(c) Application audit logs for Customer access to the Service are available for customers from the application's interface.

6. Ensuring that Personal Data is processed solely in accordance with the Instructions (control of Instructions)

(a) Anyone who is found to violate Zscaler's Code of Conduct and/or other Zscaler policies may be subject to disciplinary action including termination of employment or contract.

(b) Employees are required to sign a Non-Disclosure Agreement or other confidentiality agreement upon employment.

(c) Zscaler conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services.

(d) Zscaler maintains segmented development and production environments for all Zscaler Services, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

(e) Zscaler obtains background check reports for employment purposes. The specific nature and scope of the report that Zscaler typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law.

7. Ensuring that Personal Data is protected against accidental destruction or loss (availability control)

(a) Zscaler monitors all productions systems 24/7 to ensure the integrity of the data.

(b) Zscaler uses multiple layers of network and host-based security.

(c) Zscaler maintains disaster recovery processes to allow for continuation of data collection and to provide an effective and accurate recovery.

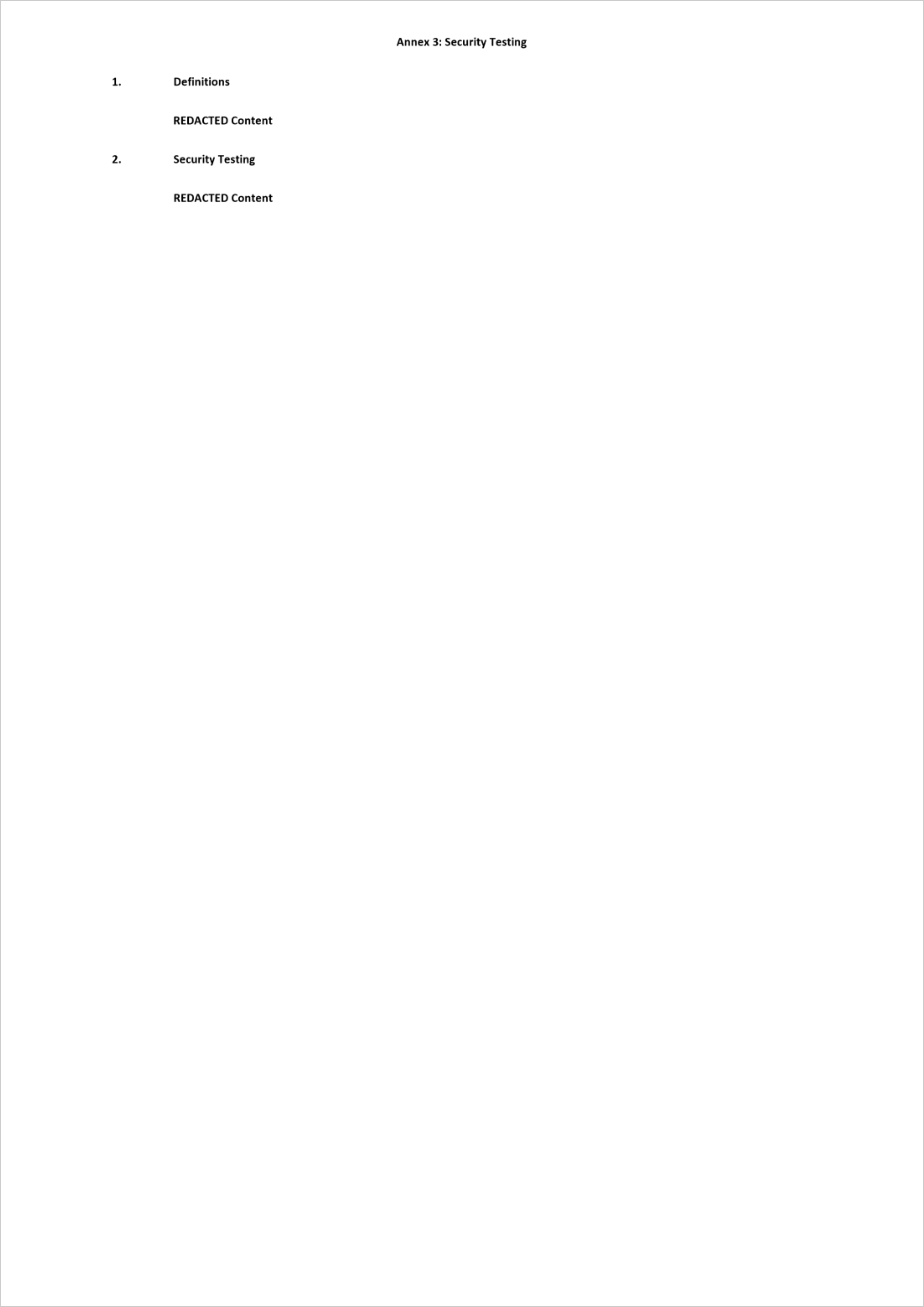
8. Ensuring that Personal Data collected for different purposes can be processed separately (separation control)

(a) Data is separated based upon Zscaler product and how it is collected. Zscaler is a multi-tenant architecture with Customer Data logically segregated. The only access to these servers and databases is via secure access by the application or via jump servers with access restricted to authorized operations personnel via multi-factor authentication.

(b) Zscaler maintains testing environments separate from production environments to avoid use of Customer Data in testing environments.

Page 28

30 June 2020 14:51



Annex 3: Security Testing

1. Definitions

REDACTED Content

2. Security Testing

REDACTED Content