Forescout Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the End User License Agreement ("EULA") or other written or electronic agreement (both collectively referred to herein as the ("Agreement") between Forescout and Customer to reflect our agreement about the processing of Personal Data (as defined in Section 1) in connection with Forescout products and services in accordance with requirements of applicable Data Protection Laws (as defined in Section 1). References to the Agreement shall include this DPA.

This DPA includes the Data Processing Terms and the attached Annexes. This DPA will be effective on the effective date of the Agreement. If Customer makes any deletions or other revisions to this DPA, and such deletions or revisions have not been expressly authorized by Forescout, then this DPA shall be null and void.

Customer	**Forescout Technologies, Inc.**
Address shall be the address of Customer as set forth in the Agreement	*Address shall be the address of Forescout Technologies, Inc. as set forth in the Agreement*
Customer's signature on the Agreement shall constitute its agreement to this DPA	***Forescout's signature on the Agreement shall constitute its agreement to this DPA***

Data Processing Terms

1. Definitions

Capitalized terms used herein and not defined have the meaning ascribed to such terms in the Agreement. The terms “**Process/Processing**,” “**Data Controller**,” “**Member State**,” “**Data Processor**,” and “**Data Subject**” will have the meanings ascribed to them in the GDPR.

“**Authorized Employees**” means Forescout’s employees or contractors who have a need to know or otherwise access Personal Data to enable Forescout to perform its obligations under the Agreement.

“**Authorized Persons**” means (i) Authorized Employees; (ii) Forescout’s contractors, consultants or partners who have a need to know or access Personal Data to perform their obligations to Customer under the Agreement; and (iii) Forescout’s Subprocessors.

“**Applicable Data Protection Laws**” means US Data Protection Laws and European Data Protection Laws that are applicable to the processing of Customer Personal Data under this DPA;

"CCPA” means the California Consumer Privacy Act of 2018, including all regulations promulgated thereunder.

“**GDPR**” means 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.

“**Forescout Services” or “Services**” means the network security solution, customer support services or any other services provided under the Agreement where Forescout Processes Customer’s Personal Data.

“**Framework**” means the Personal Data, categories of Data Subjects, activities, and security measures described in **Annex I**.

“**Personal Data**” will have the meaning ascribed to the term in the GDPR, as such Personal Data is received by Forescout by or on behalf of Customer and Processed in connection with the Forescout Services.

“**Personal Data Breach**” means a breach of security of the Forescout Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer’s Personal Data.

“**Standard Contractual Clauses**” or “**Clauses**” means the agreement by and between Forescout and Customer pursuant to the European Commission’s decision of 4 June 2021 on Standard Contractual Clauses under the European Commission’s Implementing Decision 2021/914 for the transfer of Personal Data to Data Processors established in third countries that do not ensure an adequate level of data protection.

“**Subprocessor**” means any Processor engaged by Forescout to Process the Personal Data provided by Customer to Forescout as part of the Forescout Services. For the avoidance of doubt, colocation data center facilities and transit providers are not Subprocessors under this DPA.

“**Technical and Organizational Security Measures**” or “**Security Measures”** means those measures aimed at protecting Personal Data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

2. **Applicability and Scope of this DPA**. This DPA applies only to the extent that Forescout Processes Customer’s Personal Data for the provision of Forescout’s Services.

3. Governing Terms

With respect to the Framework:

3.1. General terms and conditions of the Services are specified in the Agreement.

3.2. The Services are governed both by the terms of the Agreement and those of this DPA.

3.3. If there is a conflict between any provision or component of the Agreement and a provision or component of this DPA or the Standard Contractual Clauses as applied to the Framework, the terms of this DPA will prevail over the conflicting terms in the Agreement.

4. Details of the Processing

Customer, as a Data Controller, appoints Forescout, as a Data Processor, to Process the Personal Data on Customer's behalf as specified and instructed in the Agreement to provide Forescout Services. In some circumstances, Customer may be a Data Processor; in such case, Customer appoints Forescout as a Subprocessor. In both cases, Forescout remains a Processor with respect to Customer for the Processing activities under this DPA.

4.2 Customer agrees that it will comply with its obligations under Applicable Data Protection Laws in its collection of Personal Data, and that it has provided notice and obtained necessary consents and rights under Applicable Data Protection Laws for Forescout to process the Personal Data from the provision of Services pursuant to the Agreement.

5. Forescout's Responsibilities

5.1 Forescout shall Process the Personal Data only for the purposes set forth in the Agreement or this DPA and in accordance with the documented instructions from Customer, as modified in writing from time to time by the parties, unless required to do otherwise by applicable law to which Forescout is subject. In such a case, Forescout shall inform Customer of that legal requirement before Processing, unless that law prohibits the provision of such information on important grounds of public interest.

5.2 Forescout shall ensure that its Authorized Employees receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection, and confidentiality of the Personal Data.

6. Security

6.1 Forescout will implement and maintain appropriate Technical and Organizational Security Measures to protect against Personal Data Breaches and to preserve the security and confidentiality of Personal Data processed by Forescout on behalf of Customer in the provision of the Forescout Services. These Security Measures are subject to appropriate technical progress and development. Forescout may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Forescout Services and that Forescout shall notify Customer promptly of any materially adverse variation in the Security Measures that may threaten the security of Personal Data.

6.2 Customer agrees that it is solely responsible for its use of the Forescout Services, including securing its account authentication credentials (as applicable), and that Forescout has no obligation to protect Personal Data that Customer elects to store or transfer outside of Forescout's and Authorized Person's systems (e.g., offline or on-premises storage).

7. Subprocessors

7.1 Forescout may engage Subprocessors (including Forescout's affiliates) to provide aspects of the Forescout Services and related technical support services, provided that such Subprocessors provide sufficient guarantees to implement appropriate Technical and Organizational Security Measures substantially similar to those maintained by Forescout. Customer consents to Forescout and its affiliates subcontracting the Processing of Personal Data located in the Forescout Services to Subprocessors in accordance with this DPA and the Clauses. Any such Subprocessors will be permitted to obtain Personal Data only to deliver the services Forescout has retained them to provide, and they are prohibited from using Personal Data for any other purpose. The Subprocessors currently engaged by Forescout are identified in Annex III of this DPA. For avoidance of doubt, acceptance of this DPA serves as written acceptance of Forescout's currently engaged Subprocessors as listed.

7.2 To the extent any Subprocessors have not executed Standard Contractual Clauses (as adopted by the EU Commission through the Implementing Decision EU 2021/914 of June 4, 2021) as of the effective date of this DPA, Forescout will use reasonable efforts to execute such Clauses with such Subprocessor as soon as possible, but no later than December 27, 2022.

7.3 Forescout maintains an updated list of Subprocessors available on request by contacting privacy@forescout.com. Customer may receive notifications of new Subprocessors and updates to existing

Subprocessors by emailing privacy@forescout.com to request notifications using the process identified on the Subprocessor list in Annex III. If Customer requests notification, Forescout will notify customer if it adds any new Subprocessors at least thirty (30) days prior to allowing such Subprocessor to process Customer Personal Data. Customer may object to Forescout's appointment of a new Subprocessor within ten (10) calendar days of such notice, provided that such objection is based on reasonable grounds related to data protection. The parties will discuss such reasonable objection in good faith with a view to resolving such objections. Where an alternative cannot be made available to Customer within ninety (90) days of Customer providing notice of objection, Customer's sole remedy it to terminate the Agreement to the extent that it relates to the Forescout Services which require the use of the proposed Subprocessor.

8. Data Subjects' Requests

8.1 Forescout shall assist Customer, at no additional cost, as reasonably practicable, in the fulfilment of Customer's obligation to respond to requests by Data Subjects for exercising their rights of: access, correction, objection, erasure, and data portability, as applicable. Forescout shall respond to Customer's request for assistance in responding to a request from a Data Subject under Applicable Data Protection Laws promptly and in any event within five (5) business days after receiving Customer's written notice.

8.2 If the Data Subject makes the request directly to Forescout, Forescout shall promptly inform Customer by providing a copy of the request. Customer shall be responsible for responding to the Data Subject's request, and Forescout shall assist as set forth above.

9. Oversight.

Forescout shall deal promptly and properly with all inquiries from Customer relating to its Processing of the Personal Data.

9.1. Forescout shall make available to Customer on request information and written documents reasonably necessary to demonstrate compliance with the obligations set forth in this DPA.

9.2. Forescout shall provide written responses (on a confidential basis) to reasonable requests for information made by Customer related to Forescout's Processing of Customer's Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Forescout's compliance with this DPA, once in any twelve (12) month period or in response to a confirmed Personal Data Breach affecting Customer's Personal Data.

9.3. To the extent required by Applicable Data Protection Law, Forescout shall allow for and contribute to audits, including inspections, conducted by Customer or another auditor, as mutually agreed between the parties as required by Customer or government authorities, in relation to the Processing of Customer's Personal Data as required in the Standard Contractual Clauses. Such audits shall be limited to situations where the provided documentation as described in 9.1 and 9.2 is not sufficient to demonstrate compliance with this DPA. Customer may exercise their right to audit on reasonable prior written notice, not less than thirty (30) days in advance, during normal business hours, at Customer's expense, on the condition that Customer or Customer's third-party auditor have entered into an applicable non-disclosure agreement.

9.4. Such audit or inspection shall not require Forescout to disclose to Customer or its third-party representative any data or information on: any other Forescout customers, Forescout trade secrets, or financial matters.

9.5. An audit or inspection permitted in compliance with section 9.3 shall be limited to once in any twelve (12) month period, unless Forescout has experienced a Personal Data Breach within the previous twelve (12) months that impacted Customer's Personal Data.

9.6. Forescout shall promptly inform Customer if, in its opinion, an instruction infringes applicable law, the GDPR or other data protection provisions.

9.7. Forescout shall promptly notify Customer 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; and (ii) any request received directly from any Data Subject, without responding to that request, unless it has been otherwise authorized to do so.

10. Personal Data Breach

10.1 Forescout will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Breach") without undue delay following determination by Forescout that a Breach has occurred.

10.2 An initial report will be made to Customer security or privacy contact(s) designated in Forescout's customer support portal. As information is collected or otherwise becomes available, Forescout shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Forescout contact from whom additional information may be obtained. Forescout shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

10.3 Customer will maintain accurate contact information in the customer support portal and provide any information that is reasonably requested to resolve any security incident, including identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

10.4 Where the Standard Contractual Clauses apply, Customer will be notified in compliance with Clause 8(c) without undue delay, and within the timeframes required by the Standard Contractual Clauses.

11. Safeguards for Cross-border Transfers. Forescout will during the term of this DPA:

11.1 Maintain appropriate safeguards with respect to the Personal Data and make available to Data Subjects the rights and legal remedies with respect to the Personal Data as required under Article 46(1) of the GDPR.

11.2 Forescout relies on the Standard Contractual Clauses for cross-border transfers of data from the European Union to a country without an adequacy decision. Where Forescout makes a Restricted Transfer of Customer Personal Data from the EEA to a country without an adequacy decision, the Standard Contractual Clauses shall apply as follows:

(a) Where Customer is the Controller and Forescout is the Processor, Module Two will apply:

(i) in Clause 7, the optional docking clause will not apply;

(ii) in Clause 9(a) Option 2 General Written Authorisation will apply. The time period shall be thirty (30) days;

(iii) in Clause 11 the optional language will not apply;

(iv) In Clause 17 option 1 shall apply and will be governed by the laws of Ireland;

(v) in Clause 18 the courts shall be those of Ireland.

(vi) Annex I of the SCCs shall be deemed completed with the information set out in Annex 1 of this DPA, as applicable.

(b) Where Customer is a Processor and Forescout is a Subprocessor, the below will apply where specifically applicable in Module Three:

(i) in Clause 9 option 2 General Written Authorisation will apply. The time period shall be thirty (30) days.

11.3 For transfers of Personal Data from the UK or pursuant to the UK GDPR, the Standard Contractual Clauses EU 2010/593 shall apply, unless such SCCs cannot be used to lawfully transfer Personal Data in compliance with the UK GDPR in which case the applicable UK SCCs shall instead be incorporated by reference and form an integral part of this DPA. The general and specific references in the UK SCCs to GDPR or EU or Member State shall have the same meaning as the equivalent reference in the UK GDPR. References to the "supervisory authority" and shall mean the Information Commissioner Office, and the courts shall be those of England and Wales.

11.4 In case of any transfer of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the general and specific references in the

Standard Contractual Clauses to GDPR or EU or Member State shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws. References to the "competent supervisory authority" and courts shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland, unless such EU SCCs, cannot be used to lawfully transfer Personal Data is compliance with the Swiss DPA in which case the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes and Appendices of the Swiss SCCs shall be populated using the information in the Annexes of this DPA.

12. CCPA- No Sharing or Selling of Data for Compensation

To the extent the CCPA applies to the Parties' performance of the Agreement or to Personal Data, the parties acknowledge and agree that, with respect to the sharing of such Personal Data meeting the definition of "personal information" under the CCPA with Forescout under the Agreement, Forescout is a "service provider" as that term is defined in the CCPA. Forescout does not request or receive any Customer Data as consideration for our services or other items that we provide to Customers. We do not have, derive or exercise any rights or benefits regarding Customer Data and use Customer Data only to provide our services to Customer. We do not sell or share any Customer Data, as the terms "sell" and "share" are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act of 2020 ("CCPA"). We do not collect, retain, use, or disclose any Customer Data (a) for targeted or cross-context behavioral advertising, (b) except for the business purposes specified in a written contract with Customer, or (c) outside the direct business relationship with Customer. We do not combine Customer Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA. We will refrain from taking any action that would cause any transfers of Customer Data to or from us to qualify under the CCPA or similar laws as "sharing" for cross-contextual behavioral advertising purposes or as "selling" personal information.

13. Liability Limitation

The total combined liability of Forescout towards Customer, on the one hand, and Customer toward Forescout, on the other hand, under or in connection with the Agreement and the Standard Contractual Clauses combined will be limited to the maximum monetary or payment-based liability amount set out in the Agreement.

Remainder of Page Intentionally Left Blank

ANNEX I
Processing Details

A. LIST OF PARTIES

Controller/ Data exporter(s):

Name: The Customer. The customer's details are specified in the Agreement with Forescout for the provision of Forescout products and services.

Address: As on Agreement

Contact person's name, position and contact details: As on Agreement

Activities relevant to the data transferred under these Clauses: Provision of Forescout Services to Customer pursuant to the Agreement.

Signature and date: This annex I shall be deemed executed upon execution of the Agreement.

Role (controller/processor): Controller

Processor/ Data importer(s):

Name: Forescout Technologies, Inc.

Address: 2400 Dallas Pkwy., Plano, TX 75093 USA

Contact person's name, position and contact details: Amanda Barry, General Counsel, privacy@forescout.com

Activities relevant to the data transferred under these Clauses: Provision of Forescout Services to Data Exporter.

Signature and date: This Annex I shall be deemed executed upon execution of the Agreement.

Role (controller/processor): Processor

B. MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

1. Categories of data subjects whose personal data is transferred

- Employees, agents, advisors, independent contractors of data exporter (who are natural persons)

2. Categories of personal data transferred

- Contact information including first and last name, title, position, company, email address, phone number, physical business address
- Login and account information, including screen name, unique user ID, excluding any passwords
- Purchase history and invoicing information
- IP and MAC addresses and network topology (as applicable through a customer support case)

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

- N/A- no sensitive data will be transferred

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

- One off basis as required to provide Customer Service, fulfill the contract, or other administrative requirements
- For eyeSegment Customers the transfer will be continuous in order to provide network segmentation

5. Nature of the processing

- Forescout will Process Personal Data only as necessary to perform the Services pursuant to the Agreement, as further specified in the applicable Documentation, and as further instructed by Customer through its use of the Services

6. Purpose(s) of the data transfer and further processing

- To perform the requested Services pursuant to the Agreement

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

- The personal data will be retained for the length of the Agreement, as specified in our product documentation, or the completion of the Services

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

- A list of Forescout's Subprocessors can be found attached to this DPA as Annex III, including the details regarding the processing completed by each Subprocessor. Please contact Forescout's privacy team at privacy@forescout.com with any questions regarding our Subprocessors

C. Competent Supervisory Authority

Irish Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

Customer	**Forescout Technologies, Inc.**
Address shall be the address of Customer as set forth in the Agreement	*Address shall be the address of Forescout Technologies, Inc. as set forth in the Agreement*
Customer's signature on the Agreement shall constitute its agreement to this DPA	***Forescout's signature on the Agreement shall constitute its agreement to this DPA***

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

Data exporter is “Customer.”

Data importer

Data importer is “Forescout Technologies, Inc.”

Data subjects

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

- Employees, agents, advisors, independent contractors of data exporter (who are natural persons)

Categories of data

The categories of data are as listed on **Annex I** to this DPA.

Special categories of data (if appropriate)

The special categories of data (if any) are as listed on **Annex I** to this DPA.

Processing operations

Any basic processing activities and processing of personal data by data importer is solely for the performance of the Services as further described in the Agreement.

The personal data transferred may be subject to the following basic processing activities: collect, store, retrieve, consult, use, erase or destroy, disclose by transmission, disseminate or otherwise make available data exporter’s data as described herein, as necessary and required to provide Services in accordance with the Agreement or the data exporter’s instructions.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Scope : Forescout Cloud & eyeSegment

Description of the technical and organizational security measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Measures	Description
Measures for anonymization and encryption	Anonymization • IP addresses, MAC addresses, usernames and host names are fully anonymized o For IPV4 addresses the lower octet is hashed with a salt o For MAC addresses, the lower 3 octets are hashed with a salt o For host/usernames, one-way sha256 function is used o Data collected from Active Directory plugin is not shared with research environment Encryption • Data in transit are protected using TLS 1.2 or higher and data at rest encrypted using AES-256 algorithm • HTTPS encryption for all user interfaces using industry standard protocols and algorithms and certificates • All credentials are managed through a secure Multi factor authenticated single sign-on solution
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Forescout's eyeSegment is SOC 2 certified (2021) • Forescout's core platform is Common Criteria certified • Privacy program and ongoing training • Services are hosted in AWS o AWS's Shared Use Responsibility and AWS' SLA provide for Confidentiality, Integrity and Availability o For eyeSegment, AWS regions in US, Germany and UK are utilized o For Forescout Cloud, AWS US region is currently leveraged • Segregation of duty is enforced with strict access to production environments • Mandatory security trainings are enforced for employees that covers broad topics such as social engineering, physical security, phishing, password policies enforced under Information Security policy • Non-disclosure agreements with third parties • Network level separation and communications
Measures for ensuring the ability to restore the availability and access to	• Network Operations Center and Security Incident Response Plan

personal data in a timely manner in the event of a physical or technical incident	• All Data are populated to the cloud from the appliances. In case of data loss in the cloud, the appliance will re-send the data automatically when services are restored • Backups of Servers, Databases, and file systems • High availability and fault tolerance managed via AWS Control mechanisms
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing	• Cloud operations performs continuous scans for access threats and testing for component availability • Continuous Integration and Continuous Deployment (CI/CD) includes scans for third party vulnerabilities • Periodic penetration testing • Network level segmentation and industry leading firewalls in place • User access audits performed periodically
Measures for secure authentication and authorization	• Access Management Policy enforced for all environments • Access to production and non-production environments are protected by enforcing unique user accounts, multi-factor authentication and principle of least privilege • Access to the Forescout cloud platform via the User Interfaces and the infrastructure layer are controlled by Operations • Cloud service requires an Identity Provider and does not allow standalone access. Single Sign On configuration with multi-factor authentication o All users connected through an Identity Data Provider. • User activities logged for Create, Read, Update and Delete operations • Segregation of duty enforced with strict access to production environments • Decryption keys stored and secured in a managed system and access production data are provided only to select personnel • Keys rotated as required upon personnel rotation and/or based on a predefined calendar
Measures for the protection of data during transmission	• HTTPS encryption for data in transmission using TLS1.2 or higher • Interservice communication is protected using TLS implemented by an Istio service mesh • Leverages MTLS when need to authenticate both ends of the connection • Network is secured within AWS by leveraging Network access control lists(NACL), firewalls, AWS security groups(SG) and Secure VPN gateway
Measures for the protection of data during storage	• Data at rest are fully encrypted using industry standard AES-256 keys • Simple Storage Service (S3) encrypted with managed keys • Databases encrypted and Customer data logically and technically separated
Measures for ensuring physical security of locations at which	• AWS Cloud services ensures physical security

personal data are processed	
Measures for ensuring events logging	• Application events are monitored by NOC • AWS' CloudTrail monitors cloud events • AWS Kubernetes control plane monitors container events • User activity logged for Create, Read, Update and Delete operations
Measures for ensuring system configuration, including default configuration	• Cloud Change Management policy ensures integrity of system configurations ○ Source code and Infrastructure as Code changes tracked with detailed audit ○ Continuous Integration and Continuous Deployment (CICD) automated with auditing capabilities
Measures for internal IT and IT security governance and management	• Information Security Policy • Acceptable Use Policy • Information Classification and Protection Policy • Mobile Device Security Policy • Temporary Access Procedure • Employee Onboarding and Offboarding Procedure • Disaster Recovery Policy • Information Security Program - Policy and Compliance Management • Asset Management Policy • Personnel Security Policy • Access Management Policy • Network and Operations Security Policy • Vulnerability, Security Monitoring, and Security Incident Management Policy • Authorized software list • Physical Security Policy • System and Software Lifecycle Security Policy
Measures for certification/assurance of processes and products	• Forescout eyeSegment is SOC 2 certified (2021). • Yearly audits and maintaining compliance
Measures for ensuring data quality	• Cloud connectivity maintains associativity between appliance and cloud
Measures for ensuring limited data retention and ensuring erasure	• Data retained for operational support purposes • Data purged pursuant to retention schedule • Customer may request deletion of tenant in Cloud
Measures for ensuring accountability	• Privacy program and training • Privacy by Design in products
Measures for protecting Data Subject's rights	• Data Subjects rights requests are communicated to customers • Fulfilled through OneTrust

ANNEX III

1. Forescout Technologies, Inc. Subprocessors

The following subprocessors are authorized by Forescout Technologies, Inc. ("Forescout") to process personal data and assist in the operations necessary to provide Forescout services as described in the master services agreement:

Entity Name	Country	Type of Personal Data Processed	Purpose
Amazon Web Services	United States	IP and MAC addresses and network topology	To host customer data for certain service offerings
Oracle	United States	Contact information; Purchase history and invoicing information	To provide an ERP Tool for customer contracting and invoicing
Salesforce	United States	Contact information; Purchase history and invoicing information; Login and account information	To provide account information to Forescout in the scope of providing support to customers

2. Forescout Group Subprocessors

The following Forescout entity functions as subprocessor:

Entity Name	Country	Type of Personal Data Processed	Purpose
Forescout Technologies Israel LTD.	Israel	Contact Information; Login and account information; IP and MAC addresses and network topology	To provide support to customers as provided by customer during a support call
Forescout Technologies B.V.	The Netherlands	Contact Information; Login and account information; IP and MAC addresses and network topology	To provide support to customers as provided by customer during a support call

3. How to Subscribe to Receive a Notification of Change in Subprocessors:

If you are a current Forescout customer with a data processing agreement in place with Forescout, you may subscribe to receive notification of a new subprocessor before Forescout authorizes such subprocessor to process personal data in connection with the provision of the applicable service. You can subscribe to receive e-mail notifications for changes to the Forescout subprocessor list by emailing the following information to privacy@forescout.com:

- Customer Name
- Customer Address
- Customer E-mail
- Executed copy of the Customer-Forescout Data Processing Addendum

Please title your request "Forescout Subprocessor Notification Request."

To edit your e-mail notification information, please submit a request to privacy@forescout.com with the subject title "Change in Contact Information."