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 regarding the processing of Personal Data. This DPA describes the commitments of Forescout and Customer concerning the processing of Personal Data in connection with the use of Forescout Services. References to the Agreement shall include this DPA.

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.

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.

"**Account Data**" means information and Personal Data about Customer that Customer provides to Forescout in connection with the creation or administration of its Forescout accounts, or to complete the contracting process.

"**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; and (iii) Forescout's Subprocessors.

"**Applicable Data Protection Laws**" means European Data Protection Laws and the CCPA, where applicable to the processing of Customer Personal Data under this DPA.

"**CCPA**" means the California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020, including all regulations promulgated thereunder as amended from time to time.

"**Customer Personal Data**" means Personal Data provided by Customer to Forescout by, or on behalf of, Customer through the use of the Services. Customer Personal Data does not include Account Data.

"**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 regards to the Processing of Personal Data and on the free movement of such data.

"**Forescout Services**" or "**Services**" means the network security solutions, customer support services or Professional Services provided under the Agreement where Forescout Processes Customer Personal Data.

"**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 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 Customer Personal Data 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 Personal Data for the provision of Forescout Services.

3. Governing Terms

With respect to the Agreement:

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 Processing of Personal Data, the terms of this DPA will prevail over the conflicting terms in the Agreement.

4. Details of the Processing

4.1 Customer, as a Data Controller, appoints Forescout, as a Data Processor, to Process the Personal Data on Customer's behalf pursuant to 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 Personal Data for the Processing activities under this DPA.

4.2 Customer and Forescout agree that they are independent Data Controllers with respect to the Processing of Account Data. Forescout and Customer will comply with their obligations as a Controller and agree to provide reasonable assistance to the other party when required by Applicable Data Protection Laws.

5. Customer Responsibilities

5.1 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 and store the Personal Data for the provision of Services pursuant to the Agreement. Customer further agrees that it is responsible for: (i) reviewing the information made available by Forescout relating to security and making an independent determination as to whether the Service's meet Customer's requirements and obligations under Applicable Data Protection Laws; (ii) its secure use of the Services; and (iii) it will notify Forescout if it is unable to comply with its obligations under the Applicable Data Protection Laws or its processing instructions will cause Forescout or its Subprocessors to be in breach of such laws.

5.2 Customer is responsible for determining whether the Services are appropriate for the storage and Processing of Customer Personal Data and agrees to the extent that it controls the Personal Data provided to Forescout, it will control and limit such Personal Data to that necessary to perform the requested Services.

6. Forescout Responsibilities

6.1 Forescout shall Process the Personal Data only for the purposes set forth in the Agreement or this DPA in accordance with Applicable Data Protection Laws and 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. Forescout will notify Customer if it makes the determination that it cannot or can no longer comply with its obligations under this DPA or Applicable Data Protection Laws.

6.2 Forescout shall take reasonable steps to 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. Forescout further agrees to limit access to Customer Personal Data to Authorized Persons.

7. Security

7.1 Forescout will implement and maintain appropriate Technical and Organizational Security Measures to protect against Personal Data Breaches and to preserve the security, integrity, accessibility and confidentiality of Customer Personal Data processed by Forescout in the provision of the Forescout Services as described in Annex II. 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 promptly notify Customer of any materially adverse variation in the Security Measures that may threaten the security of Personal Data.

7.2 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 or Authorized Person's systems (e.g., offline or on-premise storage).

8. Subprocessors

8.1 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. 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. Any such Subprocessors will be permitted to obtain Customer Personal Data only to deliver the services Forescout has retained them to provide, and they are restricted from using Customer Personal Data for any other purpose.

8.2 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 via email using the process identified on the Subprocessor list in Annex III. Forescout will update the website to 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 is to terminate the Agreement to the extent that it relates to the Forescout Services which require the use of the proposed Subprocessor.

9. Data Subjects' Requests

9.1 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 after receiving Customer's written notice.

9.2 If the Data Subject makes a 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.

10. Oversight

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

10.2 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.

10.3 Forescout shall provide written responses (on a confidential basis) to reasonable requests for information made by Customer related to Forescout's Processing of Customer 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 Personal Data.

10.4 To the extent required by Applicable Data Protection Laws, 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 Personal Data as required in the Standard Contractual Clauses. Such audits shall be limited to situations where the provided documentation as described in 10.2 and 10.3 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. If the audit report includes any finding of material non-compliance with this DPA or Applicable Data Protection Laws, Customer will share the audit report with Forescout, and after Forescout's verification of the issue, Forescout will promptly cure the non-compliance.

10.5 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.

10.6 An audit or inspection permitted in compliance with section 10.4 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.

11. Cooperation

11.1 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.

11.2 To the extent required by the GDPR, Forescout shall provide reasonable assistance to Customer to allow for Customer to complete any data protection impact assessments or prior consultations with supervisory authorities as required by a supervisory authority.

12. Personal Data Breach

12.1 Upon becoming aware of a Personal Data Breach, Forescout will notify Customer without undue delay. 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 Personal Data Breach to allow Customer to notify relevant parties, including affected Data Subjects, government

agencies and data protection authorities in accordance with applicable 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 Personal Data Breach and to prevent future breaches.

12.2 Customer will maintain accurate contact information in the customer support portal and provide any information that is reasonably requested to resolve any Personal Data Breach, including to 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.

12.3 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.

13. Safeguards for Cross-border Transfers

Forescout will during the term of this DPA:

13.1 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.

13.2 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 The Republic of Ireland;

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

13.3 For transfers of Personal Data from the UK or pursuant to the UK GDPR, the Standard Contractual Clauses will apply to such transfers in accordance with Section 11.2 above with the following modifications:

(a) The EU SCCs shall be deemed amended as specified by the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under the UK Data Protection Act 2018 ("**UK Addendum**"), as may be amended, superseded or replaced, which shall be deemed executed between Forescout and Customer.

(b) Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and 11 of the UK Addendum.

(c) For the purposes of the UK Addendum, Table 1 to 3 in Part 1 shall be deemed completed using the information contained in the Annexes of this DPA.

(d) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

13.4 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.

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

To the extent the CCPA applies to the Parties' performance of the Agreement or to Customer Personal Data, Forescout agrees that it shall Process Customer Personal Data as a "service provider" as that term is defined in the CCPA. Forescout does not request or receive any Customer Personal Data as consideration for our services or other items that we provide to Customer. Forescout does not collect, retain, use, or disclose any Customer Personal Data: (i) for targeted or cross-context behavioral advertising; (ii) for any business purposes other than the purposes specified in a written contract with Customer or as permitted under the CCPA; or (iii) outside the direct business relationship with Customer. Forescout does not combine Customer Personal Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA. Forescout will refrain from taking any action that would cause any transfers of Customer Personal Data to or from Forescout to qualify under the CCPA or similar laws as "sharing" for cross-contextual behavioral advertising purposes or as "selling" personal information. Forescout agrees that it will comply with all applicable sections of the CCPA and its continued compliance with this DPA. Forescout will notify Customer if it determines that it can no longer comply with its obligations as a service provider under the CCPA. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information that is protected under the CCPA.

15. 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

FORESCOUT

ANNEX I
Processing Details

A. LIST OF PARTIES

Controller/ Data exporter(s):

Name: Customer: as 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, Suite 230, 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 as specified in the Agreement.

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)
- Users or other data subjects that are users of data exporter's network, systems, or devices
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of data exporter or use data exporter's systems, network or devices

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, and username, excluding any passwords
- IP and MAC addresses and network topology (as applicable through a customer support case)
- Device information
- Any other Personal Data submitted by, sent to, or received from Customer via the Services

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 is intended to 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 Support or Professional Services, fulfill the contract, or other administrative requirements
- transfer will be continuous during the use of the Services in order to provide cloud assisted products

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): The purchaser of Forescout's products and services.

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):

The Data Subjects are as listed on **Annex I** of this DPA

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 Personal Data as described herein, as necessary and required to provide Services in accordance with the Agreement or the data exporter's instructions.

FORESCOUT

ANNEX II

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

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 encryption	• Data is encrypted at rest and in transit using industry standard protocols and cloud platform best practices. • HTTPS encryption for all user interfaces using industry standard protocols, algorithms and digital certificates.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Forescout's products undergo yearly testing. • Services are hosted in AWS or Google Cloud Platform. • Review of security compliance certifications is completed at reasonable intervals for all third-party cloud hosting providers. • Segregation of duty is enforced with strict access to production environments. • Mandatory security trainings are enforced for employees covering topics such as social engineering, insider threats, phishing, and password policies enforced under Forescout's Information Security policy. • Non-disclosure agreements are executed with appropriate third parties. • Cloud environment access is continuously monitored using multiple tools. • The Forescout Cloud environment is configured against applicable CIS and NIST best practices and audited on a regular basis for ongoing compliance. • Third party evaluations of implemented security controls are performed annually and prior to major product revision or launch. • Network level separation and communications.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Network Operations Center and Security Incident Response Plan. • All Data is populated to the cloud from local appliances. In case of data loss in the cloud, where the appliance retains data, it will re-send the data automatically when services are restored. • Backups of Servers, Databases, and file systems are performed at regular intervals. • High availability and fault tolerance managed via Cloud Control mechanisms in the cloud environment. • Disaster recovery process is tested yearly for the Forescout Cloud platform.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing	• Cloud operations perform continuous scans for access threats and testing for component availability. • Continuous Integration and Continuous Deployment (CI/CD) includes scans for vulnerabilities in code and from third party sources. • Regular 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. • All Forescout employee credentials are managed through a secure multi factor authenticated single sign-on solution. • Customer accounts are configured with customer supplied Identity Providers, configured per their own specifications. • Access to the Forescout Cloud platform via the User Interfaces and the infrastructure layer are controlled at an organizational level by the customer. Roles are managed within the Forescout Cloud. • Cloud service requires an Identity Provider and does not allow standalone access. Single Sign On configuration with multi-factor authentication ○ All users connected through an Identity Data Provider. • User activities are logged for administration and provision actions within Forescout Cloud. • Segregation of duty enforced with strict access controls to production environments. • Decryption keys are stored and secured in a managed system and access to production data is provided only to select personnel. • Forescout managed keys are 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. • Leverages MTLS when need to authenticate both ends of the connection. • Network is secured within cloud service provider environments by leveraging access control lists, role permissions, firewalls, security groups (SG) and Secure VPN gateway.
Measures for the protection of data during storage	• GCP networks are secured leveraging Access Control Lists with role permissions. Identity Aware Proxies (IAP) and Cloud Armor (WAF) are used to secure access to internal resources. • Data at rest are fully encrypted using industry standard AES-256 keys. • Simple Storage Service (S3) and GCP buckets are encrypted with managed keys and configuration monitoring. • Databases encrypted and Customer data logically and technically separated.
Measures for ensuring physical security of locations at which personal data are processed	• Cloud services providers ensure physical security of the locations where data is stored and hosted.
Measures for ensuring events logging	• Application events are monitored by NOC. • AWS' CloudTrail monitors cloud events. • AWS Kubernetes control plane monitors container events. • GCP Stackdriver/Cloud Logging and Monitoring are monitored by Operations and Security Operations Center. • User activities are logged for administration and provisioning actions.

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	• An internal ISMS exists to maintain and update our policies to ensure that they are applicable to the needs of our customers and our business, and to ensure we are following established information security frameworks and best practices. • Our policies are verified during SOC2 audits and provide governance around acceptable use, information classification and protection, employee onboarding and offboarding, asset management, access management, network operations, vulnerability management, incident management and physical security.
Measures for certification/assurance of processes and products	• Yearly audits and maintaining compliance with industry standard certifications including applicable SOC2 Type II certifications.
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 schedules. • Customer may request deletion of tenant in Cloud environment.
Measures for ensuring accountability	• Privacy and security training for employees. • Privacy measures are considered in product design and release.
Measures for protecting Data Subject's rights	• Data Subjects rights requests are communicated to customers. • Internal measures are in place to respond to Data Subject requests in a timely manner.

FORESCOUT

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 Agreement:

Entity Name	Country	Type of Personal Data Processed	Purpose
Amazon Web Services	United States	IP and MAC addresses and network topology	Cloud hosting provider for certain service offerings
Oracle	United States	Contact information;	To provide an ERP Tool for customer contracting and invoicing
Salesforce	United States	Contact information; Login and account information	To provide account information to Forescout in the scope of providing support to customers
Google LLC	United States	IP and MAC addresses and network topology; Contact information; Account information; Other personal data provided by Customer	Cloud hosting provider for certain service offerings
Slack Technologies, LLC	United States	Contact Information; Device Information; Network topology	Internal team communications via the Slack application which may include customer support or technical incident response for Forescout Timeline and Assist
MongoDB	United States	IP and MAC addresses; Login information; User name	Managing configuration of endpoint sensors
Okta	United States	Login Information	To provide user authentication and secure MFA login to the products

2. Forescout Group Subprocessors

The following Forescout entities functions as subprocessors:

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 customer support
Forescout Technologies B.V.	The Netherlands	Contact Information; Login and account information; IP and MAC addresses and network topology	To provide customer support
Forescout Technologies (India) Private Limited	India	Contact Information; Login and account information; IP and MAC addresses and network topology	To provide customer support
Forescout Technologies Canada, Inc.	Canada	Contact Information; Login and account information; IP and MAC addresses and network	To provide customer support

		topology	
Forescout Technologies Ireland Limited	Ireland	Contact Information; Login and account information; IP and MAC addresses and network topology	To provide customer support

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

Customer 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's subprocessor list by emailing the following information to privacy@forescout.com:

- Customer Name
- Customer Address
- Customer E-mail
- 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."