EU Digital Operations Resiliency Act (DORA)

Compliance with DORA and section 13 of the EBA guidelines on outsourcing arrangements

Forcepoint

Forcepoint Products Enable Subscriber Compliance with DORA

The European Union's Digital Operational Resilience Act (DORA) regulations were implemented to ensure that certain European financial institutions can meet minimum data protection requirements with respect to regulated financial and banking information and have the ability to recover from data and network security incidents and other technological disruptions that plague our digital world today. This guide provides an understanding of how Forcepoint Products and Forcepoint Published Materials, including Forcepoint's comprehensive Product End-User Agreements included with the Forcepoint Products, Data Processing and Protection Measures, and regularly audited and certified robust security policies and practices, support our Subscribers in their achievement, maintenance, and demonstration of compliance with DORA requirements for their operations and regulated data.

How Forcepoint products support subscriber compliance with DORA requirements
Forcepoint has successfully engineered the principle of privacy by design into Forcepoint Products. As a result, Forcepoint Products do not require access to regulated financial and banking information. More information on the limited types of personal data processed by Forcepoint Products can be found in the Forcepoint Published Materials made available in the Forcepoint Customer Hub and Forcepoint Trust Hub, including the Forcepoint Product Documentation and Management of Personal Data materials.

While only processing limited types of personal data, Forcepoint Products and features can assist our Subscribers with their compliance under DORA by enhancing the security and resilience of their information and communication technology (ICT) systems.

The following table provides common use casese for Forcepoint products to demonstrate how subscribers can use Forcepoint products to achieve compliance with DORA requirements.

Forcepoint Product	Requirements
Risk-Adaptive Protection	Product Feature: Real-time risk assessment and adaptive security controls DORA Requirement: ICT Risk Management
Data Loss Preventions (DLP)	Product Feature: Data monitoring and protection against data breaches DORA Requirement: Incident Reporting and Management
Cloud Access Security Broker (CASB)	Product Feature: Visibility and control over cloud applications DORA Requirement: Third-party Risk Management
Next Generation Firewall (NGFW)	Product Feature: Advanced threat protection and network segmentation DORA Requirement: Strong Authentication and Access Control
Web Security	Product Feature: Protection against web-based threats DORA Requirement: Incident Reporting and Management
Emai Security	Product Feature: Email threat protection and encryption DORA Requirement: Incident Reporting and Management

Forcepoint published materials
More information on Forcepoint's commitment to data privacy and security can be found in the Forcepoint Trust Hub available at: https://www.forcepoint.com/legal/forcepoint-trust-hub. In addition to other guides and materials that Forcepoint has available through the Forcepoint Customer Hub, Forcepoint has also published on its public facing website:

- Forcepoint Product End-User Agreements ("FP EULA"): https://www.forcepoint.com/terms-and-conditions
- Forcepoint Data Processing and Protection Measures ("FP DPPM"): https://www.forcepoint.com/forcepoint-data-processing-agreement
- Forcepoint Data Processing Requirements ("FP DPR"): https://www.forcepoint.com/legal/data-privacy-requirements
- Forcepoint Cloud Services Service Level Agreement ("FP SLAs"): https://www.forcepoint.com/resources/legal/cloud-saas-service-level-agreement

Forcepoint supports compliance with DORA requirements
Forcepoint Products and Published Materials, including the FP EULA, FP DPPM, and regularly audited and certified robust security policies and practices, support our Subscribers in the achievement, maintenance, and demonstration of compliance with the requirements under DORA for their operations and regulated data. For example, DORA requires that in-scope European financial institutions enter into contractual agreements that are necessary to support the outsourcing of ICT services under DORA. To support compliance with this requirement while avoiding unnecessary complexities and challenges associated with an additional standalone DORA specific contract, Forcepoint has implemented the framework and guidance provided in Section 13 of the EBA Guidelines on outsourcing arrangements into the FP EULA that is included with the Forcepoint Products.

The outline and table below provide a high-level summary and more detailed description of how the Forcepoint Products and Published Materials align with the framework of Section 13 of the EBA Guidelines on outsourcing arrangements under DORA.

Forcepoint published materials and section 13 of the EBA guidelines on outsourcing arrangements

High level Summary

Written Agreements (Para 74-75):

- DORA Requirement: Clear allocation of rights and obligations in a written agreement.
- Forcepoint Compliance: The FP EULA specifies the rights and obligations of Forcepoint and its Subscribers, including Forcepoint Cloud Services SLAs, Forcepoint Technical Support service descriptions, financial obligations, and governing law.

Sub-outsourcing (Para 76-78):

- DORA Requirement: Conditions for sub-outsourcing must be specified.
- Forcepoint Compliance: The FP EULA and FP DPPM include terms related to sub-outsourcing, responsibility for compliance with data protection obligations, and the right to object to sub-processors.

IT Security Standards (Para 81-82):

- DORA Requirement: Compliance with appropriate IT security standards.
- Forcepoint Compliance: The FP DPPM incorporates ISO 27001 certified technical security measures designed to ensure robust data protection and security.

Data and System Security (Para 83-84):

- DORA Requirement: Define and monitor data and system security requirements.
- Forcepoint Compliance: The FP EULA and FP DPPM specify data protection measures, including audit rights and compliance with applicable laws.

Access and Audit Rights (Para 87-89):

- DORA Requirement: Full access and audit rights for competent authorities.
- Forcepoint Compliance: The FP EULA and FP DPPM provide audit rights, including the ability to request security assessments and audits, to help enable Subscriber compliance with legal requirements.

Termination Rights (Para 98-99):

- DORA Requirement: Clear termination provisions in case of breaches or changes.
- Forcepoint Compliance: The FP EULA includes termination rights for material breaches, and the FP DPPM allows termination if there are objections to sub-processors.

Detailed Description

Section 13	EBA Guidance	Forcepoint Agreement and Commitment
Para 74	The rights and obligations of the CLS and the service provider should be clearly allocated and set out in a written agreement.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA.
Para 75	The agreement for critical or important services should set out at least: a) a clear description of the services to be provided. b) the start date and end date, where applicable, of the agreement and the notice periods for the service provider and CLS. c) the governing law of the agreement d) the parties' financial obligations e) whether the sub-outsourcing of the service, is permitted and, if so, the conditions specified in Section 13.1 (Sub-outsourcing of critical and important services) that the sub-outsourcing is subject to. f) the location(s) (i.e. regions or countries) where the critical or important service will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the applicable FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates Forcepoint Product Documentation, the FP SLA, and the FP DPPM. Pursuant to the FP EULA, Forcepoint warrants to its Product Documentation, which specifies the features and functionalities of the Products, and provides the necessary information to allow Subscribers to control and make decisions on how to configure the Forcepoint Product, including which of the available Forcepoint Cloud Services locations to leverage and which settings and policies to deploy. The FP SLA includes service level commitments and remedies that may be available to Subscribers for missing such service levels. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub (available here:

	notify CLS if the service provider proposes to change the location(s) g) where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2 (Security of data and systems) h) the right of CLS to monitor the service provider' performance on an ongoing basis i) the agreed service levels, which should include precise quantitative and qualitative performance targets for the service to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met j) the reporting obligations of the service provider to CLS, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the service function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider k) whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested l) the requirement to implement and test business contingency plans m) provisions that ensure that the data that are owned by CLS can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider n) the obligation of the service provider to cooperate with the competent authorities and resolution authorities of CLS including other persons appointed by them o) the unrestricted right of CLS and competent authorities to inspect and audit the service provider with regard to, in particular, the services as specified in Section 13.3 (Access, information and audit rights) p) termination rights, as specified in Section 13.4 (Termination rights).	https://www.forcepoint.com/legal/forcepoint-trust-hub which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 76	The agreement should specify whether or not sub-outsourcing of the services are permitted	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM.The FP DPPM incorporates the current list of Sub-processors

		engaged by Forcepoint and specifies the rights and obligations related to such Sub-processors.
Para 77	If sub-outsourcing of critical or important services are permitted, CLS should determine whether the part of the service to be sub-outsourced is, as such, critical or important and, if so, record it in the register	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and Sub-processors engaged by Forcepoint
Para 78	If sub-outsourcing of critical or important services is permitted, the written agreement should: a) specify any types of activities that are excluded from sub-outsourcing; b) specify the conditions to be complied with in the case of sub-outsourcing; c) specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and CLS are continuously met; d) require the service provider to obtain prior specific or general written authorisation from CLS before sub-outsourcing data; e) include an obligation of the service provider to inform CLS of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set should allow the CLS to at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect; f) ensure, where appropriate, that CLS has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required g) ensure that CLS has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for CLS or where the service provider sub-outsources without notifying CLS	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM.The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. The FP DPPM specifies the obligations related to such Sub-processors, including Forcepoint's obligation to ensure that Sub-processors comply with data protection obligations tha are no less onerous than the obligations of Forcepoint in the FP DPPM (e.g., the ISO 27001 certified technical security measures that Forcepoint has in place across its organization) and the right to object to Forcepoint's use of a Sub-processor and terminate the FP EULA.

Para 79	CLS should agree to sub-outsourcing only if the subcontractor undertakes to: a) comply with all applicable laws, regulatory requirements and contractual obligations; b) grant CLS the same contractual rights of access and audit as those granted by the service provider.	Forcepoint's standard terms for vendor services incorporate the FP DPR. The FP DPR includes obligations to comply with applicable laws and secures audit rights that are sufficient to allow Forcepoint to comply with its contractual obligations to Subscribers.
Para 80	CLS should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by CLS. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important service or would lead to a material increase of risk, including where the conditions in paragraph 79 would not be met, CLS should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Sub-processors engaged by Forcepoint. The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM.The FP DPPM incorporates the current list of Sub-processors engaged by Forcepoint and specifies the rights and obligations related to such Sub-processors, including the right to object to Forcepoint's use of a Sub-processor and terminate the FP EULA.
Para 81	CLS should ensure that service providers, where relevant, comply with appropriate IT security standards	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM.The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization.
Para 82	Where relevant (e.g. in the context of cloud or other ICT outsourcing), CLS should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM.The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. The FP DPPM specifies the obligations related to such Sub-processors, including Forcepoint's obligation to ensure that Sub-processors comply with data protection obligations that are no less onerous than the obligations of Forcepoint in the FP DPPM (e.g., the ISO 27001 certified technical security measures that Forcepoint has in place across its organization).
Para 83	In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, CLS should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and the materials published in the Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub).

		The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates Forcepoint Product Documentation and the FP DPPM. Pursuant to the FP EULA, Forcepoint warrants to its Product Documentation, which specifies the features and functionalities of the Products, and provides the necessary information to allow Subscribers to control and make decisions on how to configure the Forcepoint Product, including which of the available Forcepoint Cloud Services locations to leverage and which settings and policies to deploy. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization.
Para 84	Without prejudice to the requirements under the Regulation (EU) 2016/679, institutions and payment institutions, when outsourcing (in particular to third countries should take into account differences in national provisions regarding the protection of data. CLS should ensure that agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to CLS (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM also incorporates applicable contractual commitments (e.g., the Standard Contractual Clauses) with respect to certain personal data transfers to jurisdictions that have not yet received an adequacy decision. Further, Forcepoint has published its Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 85	CLS should ensure within the agreement that the internal audit function is able to review the service using a risk-based approach.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub (available here:

		https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 86	Regardless of the criticality or importance of the service the agreement between CLS and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU with regard to service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 87	With regard to the outsourcing of critical or important services, CLS should ensure within the agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following: a) full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the service including related financial information, personnel and the service provider's external auditors ('access and information rights'); and b) unrestricted rights of inspection and auditing related to the service ('audit rights') to enable them to monitor the arrangement and to ensure	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including

	compliance with all applicable regulatory and contractual requirements.	materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 88	For the outsourcing of services that are not critical or important, CLS should ensure the access and audit rights as set out in paragraph 87(a) and (b) and Section 13.3, on a risk based approach, considering the nature of the service and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. CLS should take into account that services may become critical or important over time.	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and Forcepoint Product features and functionalities. The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates Forcepoint Product Documentation and the FP DPPM. Pursuant to the FP EULA, Forcepoint warrants to its Product Documentation, which specifies the features and functionalities of the Products, and provides the necessary information to allow Subscribers to control and make decisions on how to configure the Forcepoint Product, including which settings and policies to deploy. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 89	CLS should ensure that the agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, competent authorities or third parties appointed by them to exercise these rights	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit

		rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. The FP DPPM specifies the obligations related to such Sub-processors, including Forcepoint's obligation to ensure that Sub-processors comply with data protection obligations that are no less onerous than the obligations of Forcepoint in the FP DPPM (e.g., the ISO 27001 certified technical security measures that Forcepoint has in place across its organization).
Para 90	CLS should exercise its access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and the materials published in the Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub). The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub, which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 91	Without prejudice to their final responsibility regarding outsourcing arrangements, CLS may use: a) pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider; b) third-party certifications and third party or internal audit reports, made available by the service provider.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has

		published its Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 92	For the outsourcing of critical or important services, CLS should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and the materials published in the Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub). The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub, which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 93	CLS should make use of the method referred to in paragraph 91(b) only if they: a) are satisfied with the audit plan for the outsourced services b) ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by CLS and the compliance with relevant regulatory requirements;	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and the materials published in the Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub). The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of

	c) thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete d) ensure that key systems and controls are covered in future versions of the certification or audit report; e) are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing ,company, qualifications, expertise, reperformance/verification of the evidence in the underlying audit file); f) are satisfied that the certifications are issued and the audits are performed against widely recognised , relevant professional standards and include a test of the operational effectiveness of the key controls in place g) have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective h) retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important services	Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub, which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint's security certifications, how Forcepoint has incorporated the principle of privacy by design into the Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 94	In line with the EBA Guidelines on ICT risk assessment under the SREP, CLS should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes. CLS should also have internal ICT control mechanisms, including ICT security control and mitigation measures.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization. Further, Forcepoint has published its Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub), which has additional information on Forcepoint's commitment to data privacy and security, including materials outlining the limited types of personal data that Forcepoint processes in the provisioning of Forcepoint Products, Forcepoint policies and attestations regarding organizational and Product security, and how to request reports on Forcepoint's security assessments and audits as applicable (e.g., SOC 2 Type II).
Para 95	Before a planned on-site visit, CLS, competent authorities and auditors or third parties acting on behalf of CLS or competent authorities should provide reasonable notice to the service provider, unless this is	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of

	not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.	Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization.
Para 96	When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g., impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP DPPM specifies each party's rights and obligations with respect to the treatment and protection of personal data submitted to Forcepoint pursuant to the FP EULA, including audit rights, and incorporates the ISO 27001 certified technical security measures that Forcepoint has in place across its organization.
Para 97	Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, CLS should verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any CLS staff reviewing third-party certifications or audits carried out by service providers	To help facilitate Subscriber's compliance with its own obligations, Forcepoint will respond to Subscriber's reasonable questions related to Forcepoint Products, including those related to Forcepoint Product Documentation and the materials published in the Forcepoint Trust Hub (available here: https://www.forcepoint.com/legal/forcepoint-trust-hub).
Para 98	The arrangement should expressly allow the possibility for CLS to terminate the arrangement, in accordance with applicable law, including in the following situations: a) where the provider of the service is in breach of applicable law, regulations or contractual provisions; b) where impediments capable of altering the performance of the service are identified; c) where there are material changes affecting the arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors); d) where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information e) where instructions are given by CLS's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise CLS	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. The FP EULA references and incorporates the FP DPPM. The FP EULA and FP DPPM each reinforce the commitment to comply with applicable laws and legal requirements regarding the protection of data. The FP EULA allows for terminations for material breach and the FP DPPM allows for terminations in the event Subscriber has a reasonable basis to object to a Forcepoint Sub-processor.

Para 99	The agreement should: a) clearly set out the obligations of the existing service provider, in the case of a transfer of the services to another service provider or back to CLS including the treatment of data; b) set an appropriate transition period, during which the service provider, after the termination of the service would continue to provide the service to reduce the risk of disruptions; and c) include an obligation of the service provider to support CLS in the orderly transfer of the service in the event of the termination of the agreement	The rights and obligations of Forcepoint and Subscribers with respect to Forcepoint Products are specified in the FP EULA. The FP EULA includes the necessary terms relating to the provisioning of Forcepoint Products. Pursuant to the FP EULA, Forcepoint will provision Products for the duration of the Subscription Term, including any agreed short-term renewal Subscription Terms. Additionally, Forcepoint professional services teams are available to assist with Forcepoint Product configurations and migrations.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.