Versa Sovereign SASE und DORA-Konformität

Anforderungen an die operationale Resilienz des EU-Finanzsektors mit Versa Sovereign SASE erfüllen

Der Digital Operational Resilience Act (DORA) legt verbindliche Anforderungen dafür fest, wie Finanzunternehmen in der EU IKT-Risiken (Informations- und Kommunikationstechnologie) managen, die operationale Resilienz aufrechterhalten und Technologieanbieter überwachen müssen. Die Erfüllung dieser Vorgaben erfordert eine Infrastruktur, die sicheren Betrieb, Incident Response, Resilienztests und regulatorische Prüfbarkeit über die gesamte IKT-Umgebung hinweg unterstützt. Versa Sovereign SASE stellt einen vollständigen SASE-Stack bereit, der gezielt für regulierte Organisationen entwickelt wurde: Daten-, Control- und Management-Plane bleiben im EU-Rechtsraum, bereitgestellt als Managed Service oder im eigenen Rechenzentrum. Für Organisationen im Anwendungsbereich von DORA eröffnet Versa damit einen direkten Weg zur Compliance – ohne Abstriche bei Sicherheitsfunktionen oder betrieblicher Flexibilität, wie sie moderne kritische Infrastrukturen erfordern.

Der DORA-Rahmen

Der Digital Operational Resilience Act (DORA) (Verordnung (EU) 2022/2554), der seit dem 17. Januar 2025 in Kraft ist, schafft einen einheitlichen Rahmen für das IKT-Risikomanagement und die operationale Resilienz im gesamten EU-Finanzsektor und erfasst sowohl Finanzunternehmen als auch kritische IKT-Drittdienstleister.

DORA fasst bestehende sektorspezifische Anforderungen in einer einzigen Verordnung zusammen, die sich auf sechs Kernbereiche konzentriert:

- **IKT-Risikomanagement:** Governance, Risikorahmenwerke, Asset-Transparenz, Zugriffskontrollen, Bedrohungserkennung, Incident Response, Backup und Wiederherstellung sowie kontinuierliche Verbesserung
- **IKT-Vorfallsmanagement und -Meldung:** Definierte Prozesse zur Klassifizierung, Bearbeitung und Meldung schwerwiegender IKT-Vorfälle an die Aufsichtsbehörden
- **Tests der operationalen Resilienz:** Regelmäßige Tests von IKT-Systemen und -Prozessen, einschließlich bedrohungsorientierter Penetrationstests (TLPT) für bedeutende Unternehmen
- **Management von IKT-Drittparteirisiken:** Überwachung von Technologieanbietern, einschließlich vertraglicher Vorgaben, Prüfrechten, Konzentrationsrisiko und Exit-Strategie-Anforderungen
- **Informationsaustausch:** Freiwilliger Austausch von Cyber-Bedrohungsinformationen zwischen Finanzunternehmen
- **Aufsicht über kritische IKT-Anbieter:** Aufsicht auf EU-Ebene für Anbieter, die als systemkritisch eingestuft werden

Im Unterschied zu Vorschriften, die primär auf den Datenschutz ausgerichtet sind, zielt DORA direkt auf die operationale Resilienz ab und verlangt von Finanzunternehmen den Nachweis eines sicheren, widerstandsfähigen und prüfbaren IKT-Betriebs über ihre Netzwerke, Systeme und Drittanbieter-Technologieumgebungen hinweg.

Versa Sovereign SASE

Vor diesem regulatorischen Hintergrund bietet Versa Sovereign SASE eine Architektur, die gezielt darauf ausgelegt ist, strenge betriebliche, sicherheitstechnische und Governance-Anforderungen zu erfüllen – mit vollständigen Netzwerk- und Sicherheitsfunktionen, während Daten, Kontrolle und Betrieb innerhalb souveräner Grenzen verbleiben.

Als Bereitstellungsmodell der VersaONE Universal SASE-Plattform adressiert es eine zentrale Einschränkung herkömmlicher Cloud-SASE-Lösungen: Selbst bei lokalen Points of Presence können Traffic-Inspektion, Policy-Entscheidungen und Plattformverwaltung weiterhin von Infrastruktur außerhalb der vorgesehenen Jurisdiktion abhängen.

Versa Sovereign SASE bringt alle drei Ebenen der SASE-Architektur innerhalb einer souveränen Betriebsumgebung in Einklang:

- **Kontrollebene:** Identitätsprüfung, Policy-Auswertung und Verbindungsentscheidungen erfolgen innerhalb der festgelegten souveränen Umgebung.
- **Datenebene:** Traffic-Inspektion, Bedrohungsschutz und Content-Filterung werden an lokalen PoPs ausgeführt, ohne dass Datenverkehr zur Verarbeitung außerhalb der Jurisdiktion umgeleitet wird.
- **Management-Ebene:** Plattformverwaltung, Protokollierung, Konfiguration und operativer Zugriff bleiben lokal geregelt.

In der EU steht Versas Sovereign „SASE-as-a-Service“ zur Verfügung, wobei sämtliche Betriebs-, Datenverarbeitungs- und Support-Prozesse dem EU-Recht unterliegen – unabhängig von Versas globaler Cloud-Infrastruktur. Für Organisationen, die vollständige Infrastrukturkontrolle benötigen, ist Versa Sovereign SASE zudem für On-Premises- oder private EU-Cloud-Bereitstellungen verfügbar.

DORA-Anforderungen im Abgleich mit Versa Sovereign SASE

Die folgende Tabelle veranschaulicht, wie die Funktionen von Versa Sovereign SASE Kunden bei der Umsetzung der DORA-Anforderungen an operationale Resilienz und IKT-Risikomanagement unterstützen können.

DORA-Anforderung	Versa Sovereign SASE-Funktion	Ergebnis
Kapitel II – IKT-Risikomanagement		
Art. 5 – Governance und Organisation	Management-Dashboard mit RBAC und Aufgabentrennung; einheitliches Policy-Management über alle Sicherheits- und Netzwerkfunktionen hinweg	Unterstützt die Rechenschaftspflicht der Geschäftsleitung für IKT-Risiken durch prüfbare Governance-Kontrollen und definierte operative Rollen
Art. 5 – Governance und Organisation	VersaONE als einheitliche Plattform mit NGFW, ZTNA, SWG, IPS, ATP; zentralisierte Audit-Logs und Dashboards; alle Ebenen arbeiten innerhalb souveräner Grenzen	Unterstützt die Implementierung einer zentralisierten IKT-Risikomanagement-Architektur mit einheitlicher Sichtbarkeit und Policy-Durchsetzung
Art. 7 – IKT-Systeme, -Protokolle und -Tools	Sicheres SD-WAN mit automatischem Failover und Multipath-Resilienz; Perfect Forward Secrecy und AES-256-Verschlüsselung; geo-redundante Gateways	Unterstützt resiliente IKT-Konnektivität und sichere Kommunikation durch Redundanz und moderne kryptografische Kontrollen
Art. 8 – Identifizierung	Automatisierte Geräteerkennung und Fingerprinting; CASB-Erkennung von Schatten-IT; Anwendungssichtbarkeit mittels DPI; UEBA-Verhaltens-Baselining	Identifiziert und klassifiziert IKT-Assets, Cloud-Abhängigkeiten und anomale Zugriffsmuster zur Unterstützung des Asset- und Risikoinventars

DORA-Anforderung	Versa Sovereign SASE-Funktion	Ergebnis
Art. 9 – Schutz und Prävention	ZTNA mit kontinuierlicher Posture-Bewertung; MFA; DLP mit vordefinierten Mustern (PII, DSGVO, PCI-DSS); GenAI Firewall; SWG; lokalisierte Kontrollebene mit Zugriffsentscheidungen innerhalb souveräner Grenzen	Setzt Least-Privilege-Zugriff, starke Authentifizierung und Datenschutzkontrollen durch, wobei Policy-Entscheidungen vollständig innerhalb der souveränen Umgebung getroffen werden
Art. 10 – Erkennung	UEBA mit KI-gestützter Anomalieerkennung; ATP mit Multi-AV, KI/ML und Sandboxing; NG-IPS; DNS-Tunnel-Erkennung; DEM für Performance-Anomalien; durchgängige Zuordnung zu MITRE ATT&CK	Bietet kontinuierliche Echtzeit-Erkennung von Bedrohungen und IKT-Anomalien mit strukturierter Klassifizierung entlang eines standardisierten Bedrohungs-Frameworks
Art. 11 – Reaktion und Wiederherstellung	Automatisches SD-WAN-Failover; geo-redundante Gateways mit Active-Active-HA; ATP-Eindämmungsmaßnahmen; Mikrosegmentierung zur Begrenzung des Schadensradius; Wiederherstellungsmaßnahmen werden innerhalb der souveränen Management-Ebene gesteuert	Unterstützt schnelle Eindämmung, Reaktion und Wiederherstellungsabläufe innerhalb der Grenzen des jeweiligen Rechtsraums
Art. 12 – Backup- und Wiederherstellungsverfahren	Konfigurations-Backup und -Wiederherstellung; lokalisierte Protokollierung und Konfigurationsdaten innerhalb der souveränen Management-Ebene	Unterstützt die Wiederherstellung von Netzwerk- und Sicherheits-Policies, wobei Backup-Daten im souveränen Rechtsraum gespeichert werden
Art. 13 – Lernen und Weiterentwicklung	UEBA- und ATP-Zuordnung nach Vorfällen gemäß MITRE ATT&CK; kontinuierliche Aktualisierung der Bedrohungsdaten-Feeds; zentralisierte Sicherheitsberichte und Dashboards	Ermöglicht eine strukturierte Nachbetrachtung von Vorfällen und die kontinuierliche Verbesserung der IKT-Risikokontrollen auf Basis aktueller Bedrohungsinformationen
Art. 14 – Kommunikation	Zentralisierte Alarmierung und Berichterstattung; SIEM-Integration über IPFIX, Syslog und VMS	Liefert zeitnahe, strukturierte Sicherheitsereignisdaten zur Unterstützung interner und externer Krisenkommunikationsprozesse
Kapitel III – IKT-Vorfallsmanagement und -Meldung		
Art. 17 – Prozess für das Vorfallsmanagement	Echtzeit-Alarmierung durch UEBA und ATP mit automatisierter Klassifizierung; NG-IPS- und DNS-Sicherheitsereignisprotokolle; SIEM-Streaming über IPFIX, Syslog, NetFlow und PCAP; modulbezogene Dashboards	Unterstützt Frühwarnung, strukturierte Dokumentation von Vorfällen und definierte Reaktionsrollen zur Erfüllung der DORA-Anforderungen an das Vorfallsmanagement
Art. 18 – Klassifizierung von Vorfällen	DEM zur Quantifizierung betrieblicher Auswirkungen; Schweregrad-Bewertung durch ATP und UEBA mit MITRE-ATT&CK-Zuordnung; dienstbezogene Berichterstattung	Liefert strukturierte Schweregrad- und Auswirkungsdaten zur Unterstützung der Klassifizierung IKT-bezogener Vorfälle gemäß DORA-Kriterien
Art. 19 – Meldung schwerwiegender Vorfälle	Umfassende Protokollierung über IPFIX, Syslog, NetFlow und PCAP; SIEM-Integration über VMS; sämtliche Logdaten werden im souveränen Rechtsraum gespeichert und verarbeitet	Bietet zentralisierte Protokollierung zur Beweissicherung und für regulatorische Meldeprozesse, bei durchgängiger Logverarbeitung innerhalb des souveränen Rechtsraums

DORA-Anforderung	Versa Sovereign SASE-Funktion	Ergebnis
Kapitel IV – Tests der digitalen operationalen Resilienz		
Art. 24–25 – Tests der digitalen operationalen Resilienz	ZTNA-Netzwerksegmentierung für kontrollierte Testumgebungen; RBAC zur Trennung von Test und Produktion; MITRE-ATT&CK-Zuordnung für das Test-Scoping; ATP- und IPS-Baseline-Daten für Schwachstellenanalysen	Ermöglicht strukturierte Resilienz- und Schwachstellentests mit kontrolliertem Schadensradius und dokumentierter Konfigurationshistorie für die Lückenanalyse
Art. 26 – Bedrohungsorientierte Penetrationstests (TLPT)	MITRE-ATT&CK-basierte Bedrohungsdaten für das Test-Scoping; ZTNA-Mikrosegmentierung für isolierte Testumgebungen; TLPT-Telemetrie und -Ergebnisse verbleiben innerhalb der souveränen Grenzen	Unterstützt TLPT-Aktivitäten durch isolierte Testumgebungen und lokalisierte Telemetrieverarbeitung innerhalb souveräner Bereitstellungsmodelle
Kapitel V – Management von IKT-Drittparteirisiken		
Art. 28 – Management von Drittparteirisiken	Cloud- und SaaS-Transparenz und -Kontrolle: Erkennung von Schatten-IT, Posture-Überwachung und API-basierte Datensicherheit; Sovereign-SASE-as-a-Service innerhalb der EU-Jurisdiktion	Deckt IKT-Abhängigkeiten von Drittanbietern auf und überwacht diese, während EU-geregelte vertragliche und operative Vereinbarungen für kritische Netzwerk- und Sicherheitsdienste unterstützt werden
Art. 29 – IKT-Konzentrationsrisiko	Einheitliche Posture-Transparenz über die gesamte Cloud-Service-Landschaft; Sovereign-SASE-Architektur, die unabhängig von der globalen, gemeinsam genutzten Infrastruktur von Versa betrieben wird	Bietet operative Transparenz, souveräne Bereitstellungsoptionen und reduzierte Abhängigkeit von global geteilter Infrastruktur
Art. 30 – Wesentliche Vertragsbestimmungen	Sovereign SASE-as-a-Service mit EU-geregeltem Betrieb, lokalisierter Datenverarbeitung und Support; RBAC und Audit-Trail zur Unterstützung von Prüfrechten; lokale Kontroll-/Management-Ebene mit überprüfbaren operativen Zugriffskontrollen	Unterstützt DORA-Vertrags- und Aufsichtsanforderungen durch EU-geregelten Betrieb, lokalisierte Verarbeitung, Audit-Protokollierung und operative Zugriffskontrollen
Art. 31–44 – Aufsicht über kritische IKT-Anbieter	Sovereign SASE, vertraglich über eine EU-Rechtseinheit mit lokalisiertem Betrieb bereitgestellt; Protokollierung und Audit-Trail zur Unterstützung regulatorischer Auskunftsersuchen; EU-geregelter Support und operative Ansprechpartner	Liefert dokumentierte Nachweise des Betriebsmodells zur Unterstützung regulatorischer Bewertungen und Aufsichtsprüfungen
Kapitel VI – Informationsaustausch		
Art. 45 – Informationsaustausch	Bedrohungsdaten-Feeds (Dateireputation, DNS, ATP); SIEM-Streaming über IPFIX, Syslog und VMS; MITRE-ATT&CK-Ausrichtung für standardisierten Bedrohungsaustausch; Bedrohungstelemetrie verbleibt innerhalb der souveränen Jurisdiktion	Ermöglicht die Teilnahme an branchenweiten Vereinbarungen zum Bedrohungsaustausch und minimiert gleichzeitig grenzüberschreitende Telemetrieübermittlungen

Warum DORA-regulierte Organisationen auf Versa setzen

DORA-Konformität erfordert eine Infrastruktur, die operative Kontrolle, Resilienz und Prüfbarkeit über den gesamten Netzwerk- und Sicherheits-Stack hinweg nachweisen kann. Als First-to-Market-Anbieter für Sovereign SASE liefert Versa ein Bereitstellungsmodell, das gezielt für regulierte Organisationen entwickelt wurde, die operative Unabhängigkeit und souveräne Kontrolle benötigen.

Zentrale Gründe, warum sich Finanzunternehmen für Versa Sovereign SASE zur DORA-Konformität entscheiden:

- **Vollständige Souveränität im gesamten Stack:** Daten-, Kontroll- und Management-Ebenen verbleiben innerhalb EU-gehosteter und -kontrollierter Infrastruktur
- **Vollständige SASE-Funktionen:** Integrierte ZTNA-, NGFW-, SWG-, CASB-, DLP-, IPS-, ATP- und SD-WAN-Funktionen innerhalb souveräner Umgebungen
- **Prüfbare Governance:** Protokollierung, RBAC und SIEM-Integration unterstützen regulatorische Berichterstattung und die Überwachung von Drittanbietern
- **Flexible Bereitstellung:** Verfügbar als Managed Service, On-Premises-Bereitstellung oder private EU-Cloud-Bereitstellung

Fordern Sie eine Demo an, um Versa Sovereign SASE in Aktion zu sehen.

Entdecken Sie Versa Sovereign SASE.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
info@versa-networks.com
www.versa-networks.com

Über Versa

Versa, ein globaler Marktführer im Bereich SASE, ermöglicht es Organisationen, selbstschützende Netzwerke aufzubauen, die ihre Netzwerk- und Sicherheitsinfrastruktur radikal vereinfachen und automatisieren. Die KI-gestützte VersaONE Universal SASE Plattform bietet konvergente SSE-, SD-WAN- und SD-LAN-Lösungen, die Daten schützen und vor Cyberbedrohungen verteidigen und dabei ein hervorragendes digitales Nutzererlebnis liefern. Tausende Kunden weltweit, mit Hunderttausenden Standorten und Millionen Nutzern, vertrauen Versa ihre unternehmenskritischen Netzwerke und ihre Sicherheit an.

©2026 Versa Networks, Inc. Alle Rechte vorbehalten. Teile der Versa-Produkte sind durch Versa-Patente sowie angemeldete Patente geschützt. Versa Networks und FlexVNF sind Marken oder eingetragene Marken der Versa Networks, Inc. Alle anderen hierin verwendeten oder erwähnten Marken sind Eigentum ihrer jeweiligen Inhaber. Teil-Nr. SB_SOV-SASE-DORA-CMP-01.0