EU General Data Protection Regulation (GDPR) – Reference Card

The EU GDPR is effective from 25 May 2018, and it is the culmination of years of work by the EU to reform Data Protection regulation into a Union-wide framework instead of a patchwork of country-specific legislations. The GDPR affects all organizations that hold personal data on EU citizens, regardless of where the organization is based in the world. The maximum fines for non-compliance are the higher of €20m and 4% of the organization's worldwide turnover. This document describes how Sophos products can be effective tools to help address some of the requirements as part of a customer's efforts to comply with GDPR.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

Requirement	Sophos solution	How it helps
Undertake a comprehensive risk assessment	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk level and prioritize response. Average time to detect and investigate is just 26 minutes.
Manage and control network security to protect personal data residing in systems and applications	Sophos Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Synchronized Security feature in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos Managed Detection and Response (MDR)	Threat-hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high-caliber, actional signals across the network infrastructure to optimize cyber defenses.
	Sophos Switch	Allows configuration of VLANs to segment your internal traffic and reduce the attack surface in case of an infection or breach. Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
Protect personal data at rest	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive personal data and can prevent leaks of such information via email, uploads, and local copying.

SOPHOS

Requirement	Sophos solution	How it helps
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
Protect personal data in transit	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
	Sophos Firewall	Allows for policy-based encryption for VPN tunnels, protecting data in transit.
	Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
Protect data against viruses and other malware	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated and correlated to identify malicious activities and enable us to quickly neutralize the event.

Requirement	Sophos solution	How it helps
	Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
Establish processes to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources	Sophos Firewall	Instantly identifies the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	24/7 detection and neutralization of malicious software by human experts, leveraging AI, technologies, and threat expertise.
Allow only authorized access to personal data	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
	Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
	Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
Implement protection against data leaks	Sophos Intercept X Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Email	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help ensure compliance.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.

Requirement	Sophos solution	How it helps
	Sophos Firewall	Limits access between untrusted devices and critical servers with the segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain. Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
Quickly detect, investigate, and send notifications of personal data breach	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a dedicated team of response specialists who are experts at battling adversaries. Clear procedures and documentation enable consistent info sharing.
Respond to security incidents within the stated time period	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. The average time to detect, investigate and respond is just 38 minutes. Clients choose the level of response they wish us to take.
Audit current compliance position against the GDPR's requirements	Sophos Cloud Optix	Continuously monitor compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. Automatically analyze cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps leaving you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2022-11-23 CC (PC)

SOPHOS