SOPHOS
Cybersecurity made simple.

GDPR Compliance for Schools

The General Data Protection Regulation (GDPR) became effective on May 25, 2018 and significantly changed the way personal data is handled in the EU and beyond. GDPR provides more stringent protection requirements than its predecessor, the 1995 Data Protection Directive, and this new law will affect all schools in the EU that hold personal data. The maximum fines for non-compliance are €20 million or 4% of an organization's worldwide turnover, whichever is higher.

For schools, the job of securing data is becoming ever harder. Students and staff have multiple devices all containing data that is important to the school. What makes it even tougher is that students and staff want to be able to work with this data wherever they are and with whatever device they choose. For a school, it's incredibly challenging to lock down and secure this information, especially when we want to enable staff and students to maximize their learning potential and not hold them back through restrictive policies.

Over 12,000 schools trust Sophos to help them secure their data. Working with our education partners, we have put together a list of some important considerations a school should consider when working towards complying with GPDR. We also explain how our technology can support your GDPR compliance efforts.

□ Build your data map

Understand what personal data you process, where it came from, how it's used, and who it can be shared with. Once you understand the data you have and where it can go, you'll be in a better position to build processes and policies to protect it and to choose the right technologies to help keep it secure.

□ Build your privacy policy and disclose it to individuals

Now that you understand the data you have and how you handle it, it's time to build your privacy policy. Your privacy policy explains to individuals how you process their personal data, including your lawful bases for doing so, what data you process, your data retention periods, and the rights that those individuals have with respect to their data. Keep in mind that your policy must be simple to understand by all. In some cases, you may need consent from a child's parent or guardian to collect that child's personal data, and you should plan how you will obtain that consent in a GDPR-compliant manner.

Important points to remember when drafting your data protection policy:

- Cleansing and consolidation of legacy data
- Pseudonymizing and anonymizing data you are legally obliged to retain
- Subject access requests
- The right to be forgotten
- Privacy by design for collection of all future data
- Process to report data breaches

□ Secure your personal data

GDPR requires all organizations, including schools, to implement appropriate measures to ensure personal data is secured. GDPR does not prescribe specific technical measures schools need to adopt, but Sophos offers a wide and comprehensive range of options that you can choose from as you work to build security infrastructure to protect data throughout your organization. Deploy security technology to stop attacks and malicious traffic at your network perimeter and protect data on your endpoints and servers. Sophos XG Firewall can help you stop advanced malware attacks before they can hit your network and also prevent attacks from spreading. Sophos Intercept X keeps your endpoints and servers secure from the latest malware and ransomware.

□ Secure data on devices

Keep your data secure if a device is lost or stolen. Sophos Central Device Encryption offers the easiest way to manage full-disk encryption on PCs and Macs that secures your devices so that data on them is protected even if lost or stolen. Sophos Mobile protects data on mobile devices and offers comprehensive anti-theft and loss protection.

□ Reduce the impact of human error

Train your students and staff to identify malicious emails. Sophos Phish Threat can help you send simulated phishing emails to users, testing their susceptibility to attacks and providing them with training.

Keep individual files secure wherever they go and prevent unintentional disclosure. Sophos SafeGuard offers next-gen file encryption to keep your data safe even when it leaves your network and devices. It automatically and seamlessly encrypts and decrypts files as they are uploaded or downloaded from public cloud storage devices like Dropbox and OneDrive. Always-on Synchronized Encryption ensures all files are always encrypted everywhere.

□ Document your data processing activities

Keep a written record of your data processing activities, including documenting the lawful bases for your processing of personal data, the categories of personal data held, the retention policy for this data, the security measures you undertake to protect this data, and other relevant information. You might be required to make this information available to a data protection authority when asked.

□ Only collect as much personal data as is required, and keep it for as long as required

You should minimize the amount of personal data your school collects, based on what you need it for. Set up a data retention policy and engage in periodic reviews to identify and delete or anonymize data when it ceases to be of valid use to your school.

□ Communicate with internal stakeholders and staff

GDPR is important and the potential penalties for non-compliance are hefty. Your users and school's senior management team need to fully understand the new procedures around GDPR as well as the compliance obligations that it entails for your school.

EU General Data Protection Regulation (GDPR) – Reference Card

REQUIREMENT	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
Stop hacking and malware		
Stop attacks and malicious traffic at your network perimeter	**XG Firewall**	Stops advanced malware attacks before they can hit your network and stops attacks from spreading.
Protect data on your endpoints	**Intercept X**	Keeps your endpoints secure from the latest malware and ransomware.
Automated, faster threat response	**Intercept X** **XG Firewall**	Synchronized Security shares data between the firewall and endpoints to automatically identify and isolate compromised systems.
Protect data on your servers	**Server Protection**	Keeps your s secure from the latest malware and ransomware.
Secure lost or stolen devices		
Keep your data secure if devices are lost or stolen	**Sophos Central Device Encryption**	The easiest way to manage full disk encryption on PCs and Macs that secures your devices so data on the disk is always safe even if lost or stolen.
	Sophos Mobile	Protects data on mobile devices and includes comprehensive anti-theft and loss prevention.
Reduce impact of human error		
Train users to identify malicious emails	**Phish Threat**	Sends simulated phishing emails to users, testing susceptibility to attacks. Trains them on key things to look for.
Keep individual files secure wherever they go	**Sophos SafeGuard**	Next-gen file encryption keeps your data safe even when it leaves your corporate network and devices.
Protect sensitive data in the cloud	**Sophos SafeGuard**	Automatically and seamlessly encrypt and decrypt files as they are uploaded or downloaded from public cloud storage services like Dropbox and OneDrive.
Prevent unintentional disclosure	**Sophos SafeGuard**	Synchronized Encryption that is always on makes sure all files are always encrypted everywhere.
Stop sensitive files being sent by mistake	**Sophos Central Endpoint Advanced**	Stops sensitive keywords in documents or specific file types from leaving the endpoint.

GDPR Enforcement

GDPR is of global interest as it impacts many organizations doing business with European residents – regardless of where the organization is based. GDPR greatly strengthens enforcement powers of regulators. The new maximum fines of €20 million or 4% of annual worldwide turnover (whichever is higher) demonstrate a significant increase on previous fines, which means the consequences of a breach have become much more significant.

DISCLAIMER/IMPORTANT NOTICE

The information in this document is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. While we hope the information in this document will be useful, Sophos assumes no responsibility for the information contained in this document and disclaims all liability in respect of such information.

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

Oxford, UK

SOPHOS