SOPHOS
Cybersecurity made simple.

Sophos Transfer Risk Assessment

Completed January 2022

About the Personal Data

Type and Categories of personal data	As described in the Product Data Sheets available on the Sophos Trust Center at https://www.sophos.com/en-us/trust/privacy.aspx

About the Transfer

Types of entities involved in the transfer	Sophos Limited is a data exporter transferring personal data to Sophos entities outside of the EU for purposes of providing Sophos products and services. Sophos Limited also engages third party suppliers for purposes of delivering products and services to customers.
Sector in which the transfer is occurring	Cyber-security
Purpose of the transfer	Provision of product and support related services to customers requires international data transfers to and between Sophos Limited (UK) and Sophos entities outside of the EU.
Method of transfer	Sophos uses remote access to data where necessary, for purposes of providing technical support and customer support services to its customers.
Storage location of data	Sophos products and services are provided from an EU-located data centre. In few instances the location of data storage may vary by product and is set out in the relevant data sheets in our Trust Center: https://www.sophos.com/en-us/legal/product-privacy-information
Sophos non-EU entities for purposes of personal data transfers	Sophos Inc (USA) Sophos Technologies Private Limited (India) Sophos Pty (Australia)

Likelihood of Third Party Access

Sophos entities based outside of the EU may provide necessary support and other product-specific services to Sophos Limited to enable it to undertake its obligations to customers and partners.

In some instances Sophos may occasionally enable third party access where such third parties:

1) Provide necessary support and other services to Sophos to enable it to undertake its obligations to customers and partners. Sophos sub-processors are listed at https://www.sophos.com/en-us/legal/sub-processor. In rare instances where such a third party should need to access personal data, such access will be governed by appropriate Non-Disclosure and Data Processing Agreements.
2) Are empowered by law to request access to such data, such as law enforcement agencies. Whenever a request is received, it will be subject to full validation and review internally.

Country-Specific Matters

United States of America: Although it is possible that Sophos Inc may be subject to FISA 702, it is unlikely that Sophos products and/or services are of interest to U.S. Government Agencies. In any event, Sophos Limited applies additional security measures including encryption, organisational and business continuity controls, which are detailed in the appendix below.

Risk of Harm to Data Subjects

There may be a risk of harm to data subjects based on unlawful access to personal data. This could materialise by unlawful access made by third party vendors / suppliers, malicious attack or unauthorised access to data. Sophos has robust security procedures in place to protect against malicious attack, to properly review and scrutinise vendors as well as procedures to mitigate unauthorised access to data. The destination countries which include the United States predominantly, present no inherent greater risk of unlawful access being made.

Risk Assessment

The transfer of personal data to Sophos Inc is a necessary part of providing products and services to Sophos customers.

International Data Transfer Agreements with appropriate Standard Contractual Clauses are implemented between Sophos Limited (Exporter) and Sophos Inc (Importer) as well as between Sophos and its third party suppliers and these set out the necessary data protection measures in place related to the transfer and onward processing of data. Furthermore Sophos enters into intragroup data transfer agreements between its entities and these are also bolstered by the Standard Contractual Clauses to ensure that its data transfer complies with applicable European and United Kingdom laws.

This arrangement is deemed likely to be enforceable in the destination countries.

Third party access to data is strictly limited by access controls and data subjects are informed by way of the Privacy Notice about the third party processing that may occur.

The residual risk to data subjects as a result of this transfer are considered to be low and a significant risk of harm does not appear to be presented. Based on this assessment, the protection measures set out in the International Data Transfer Agreement and Standard Contractual Clauses are deemed sufficient to limit the risk of harm to data subjects.

SOPHOS
Cybersecurity made simple.

Appendix A
Security Measures adopted by data Importer

A) Physical Access Control.

- Sophos has a physical access control policy;
- All staff carry ID / access badges;
- Entrances to facilities are protected by access badges or keys;
- Facilities are divided into (i) public access areas (such as reception areas), (ii) general staff access areas, and (iii) restricted access areas which may only be accessed by those personnel with an express business need;
- Access badges and keys control access to restricted areas within each facility according to an individual's authorised access levels;
- Access levels for individuals are approved by senior staff members and are verified on a quarterly basis;
- Reception and/or security staff are present at entrances to larger sites;
- Facilities are protected by alarms;
- Visitors are pre-registered and visitor logs are maintained.

B) System Access Control.

- Sophos has a logical access control policy;
- The network is protected by firewalls at each Internet connection;
- The internal network is segmented by firewalls based on application sensitivity;
- IDS and other threat detection and blocking controls run on all firewalls;
- Filtering of network traffic is based on rules that apply the principle of "least access";
- Access rights are only granted to authorised personnel to the extent and for the duration necessary in order to perform their job roles and are reviewed quarterly;
- Access to all systems and applications is controlled by a secure log-on procedure;
- Individuals have unique user IDs and passwords for their own use;
- Passwords are strength tested and changes are enforced to weak passwords;
- Screens and sessions automatically lock after a period of inactivity;
- Sophos malware protection products are installed as standard;
- Regular vulnerability scans are conducted on IP addresses and systems;
- Systems are patched on a regular cycle with a prioritisation system for fast-tracking urgent patches.

C) Data Access Control.

- Sophos has a logical access control policy;
- Access rights are only granted to authorised personnel to the extent and for the duration necessary in order to perform their job roles and are reviewed quarterly;
- Access to all systems and applications is controlled by a secure log-on procedure;
- Individuals have unique user IDs and passwords for their own use;
- Passwords are strength tested and changes are enforced to weak passwords;
- Screens and sessions automatically lock after a period of inactivity;
- Laptops are encrypted using Sophos encryption products;
- Senders are directed to consider file encryption prior to sending any external email.

D) Input Control.

- Access to all systems and applications is controlled by a secure log-on procedure;
- Individuals have unique user IDs and passwords for their own use;
- The Sophos Central Products use transfer layer encryption to protect data in transit;

- Communication between the client software and the backend Sophos system is performed over HTTPS to secure the data in transit, establishing trust communication via certificates and server validation.

E) Subcontractor Control.

- Subcontractors with access to data undertake an IT security vetting procedure prior to onboarding and as required thereafter;
- Contracts contain an appropriate confidentiality and data protection obligations based on the subcontractor's duties.

F) Availability Control.

- Sophos protects its premises from fire, flood and other environmental hazards;
- Back-up generators are available to maintain power supplies in the event of power outages;
- Data centres and server rooms use climate controls and monitoring;
- The Sophos Central system is load balanced and has failover between three sites, each running two instances of the software, any one of which is capable of providing the full service.

G) Segregation Control.

- Sophos maintains and applies a quality control process for the deployment of new customer products;
- Testing and production environments are separate;
- New software, systems and developments are tested prior to release to the production environment.

H) Organisational Control.

- Sophos has a dedicated IT security team;
- The Risk and Compliance team manage internal risk reporting and controls, which include reporting on key risks to management;
- An incident response process identifies and remedies risks and vulnerabilities on a timely basis;
- Each new employee undertakes data protection and IT security training;
- The IT Security department conducts quarterly security awareness campaigns.

Date of assessment	21st February 2022
Date of next review	31st August 2022