SKOUT
CYBERSECURITY

SKOUT CYBERSECURITY PRIVACY DATA SHEET

Overview

SkOUT values our customer's privacy and is dedicated to our customer's security. We believe it's impossible to be secure unless you can maintain privacy, in line with recently enacted Data Protection legislation, namely the Data Protection Act 2018 and the GDPR. With this in mind, SkOUT architected NeverBlink™ to enable a high degree of privacy and security for our customers.

This data is stored in the SkOUT EMEA AWS Cloud Service which is located in Europe and is separate from the customer's tenant. While data contained within executable binaries is generally non-personal, any attribution data is de-identified prior to analysis. We never share these files with any third party, or even internal parties that don't have an absolute need to know. Customers select the location of their tenant instances, and no personal data is transferred to other geographies without instructions from the customer. Some nonpersonal data may be transferred to the United States to improve the performance and efficacy of the product. The SkOUT information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish an access control capability throughout SkOUT and its business units to help the organization implement security best practices with regard to logical security, account management, and remote access.

Personal Data Processed

The nature and purpose of the Processing of Client Personal Data by the SkOUT is the performance of the Services pursuant to the Agreement (cyber security monitoring and professional services).

Personal Data Processed	Purpose of Processing
Names, Email addresses, Log in IDs, User IDs, payment information	• Deliver service • Billing and invoicing • Customer support
Digital ID: IP addresses, Hostname, MAC addresses	• License management • Contract management • Identify and protect against threats
Traffic Pattern: Destination addresses of web browsing (does not include content)	• Identify and protect against threats

Data Sharing or Transferring With 3rd Parties

NeverBlink™ does not share customer's data with third parties. SkOUT uses Amazon Web Services (AWS) and Citrix ShareFile as sub-processors to deliver the service to the customer. The scope of this policy is applicable to all Information Technology ("IT") resources owned or operated by SkOUT.

Cross-Border Data Transfers

SkOUT's customers select the geographic location for their tenant, which is where personal data used to manage their service, along with data collected from endpoints, is stored. Data is not transferred from the chosen customer's tenant location to any other geography without customer instruction.

getskout.com
info@skoutsecure.com

EMEA Office
IDA Business and Technology Park
Unit 1, Mountrath Road, Portlaoise
Co. Laois. Eircode: R32 CA44
+353 1 660 0800

Security Operations North America
270 South Service Road
Suite 55
Melville, NY 11747
+1 631 203 6600

Corporate Office
423 West 55th Street
7th Floor
New York, NY 10019
+1 631 203 6600

© 2019 SKOUT SECURE INTELLIGENCE
PROPRIETARY AND CONFIDENTIAL

Customer Tenant Geography	Location	Sub-Processor
United States	New York	Amazon Web Services
Europe	Ireland, UK	

Data Retention*

Personal Data Processed	Data Retention Period
Customer Contact Information	No fixed retention periods. Personal data may be deleted upon request
Endpoint Data	Data is removed at the end of the contract
Customer Administrative Login Activity	Data is removed at the end of the contract

* Data Retention Period as noted, unless otherwise required by applicable law or regulatory authority.

getskout.com
info@skoutsecure.com

EMEA Office
IDA Business and Technology Park
Unit 1, Mountrath Road, Portlaoise
Co. Laois. Eircode: R32 CA44
+353 1 660 0800

Security Operations North America
270 South Service Road
Suite 55
Melville, NY 11747
+1 631 203 6600

Corporate Office
423 West 55th Street
7th Floor
New York, NY 10019
+1 631 203 6600

© 2019 SKOUT SECURE INTELLIGENCE
PROPRIETARY AND CONFIDENTIAL