netskope

Netskope Cloud Risk Assessment for the EU General Data Protection Regulation (EU GDPR)

An analysis of your organisation's cloud app usage and compliance with the pending EU GDPR.

The Netskope CRA for the EU GDPR will discover cloud apps in your organisation, their likely compliance with the EU GDPR, and recommend actions and policies for compliance.

What is the Netskope Cloud Risk Assessment (CRA) for the EU GDPR?

Organisations are adopting cloud apps at a rapid pace. Whether you allow or block these apps, chances are your users have found a way to access them. With the European Commission developing hard-hitting legislation to protect privacy data that will carry heavy fines and supersede all other privacy regulations, you need visibility into your organisation's cloud app usage so you can know your areas of likely non-compliance and ready yourself to comply with this pending law. The assessment will provide you an overview of your cloud apps, how enterprise-ready they are, and their likely compliance with the EU GDPR, as well as recommendations for being compliant with the regulation. It can provide a basis for which areas your organisation needs to address to be cloud-compliant with the GDPR.

What is included in the Netskope CRA for the EU GDPR?

Netskope offers two CRA types, Standard and Advanced. The table below outlines

WHAT'S INCLUDED	STANDARD	ADVANCED
Secure, dedicated Netskope tenant instance	Secure, dedicated tenant, no access	Secure, dedicated tenant, access for 1 month
Discovered apps by category	Top categories only	Summarised for all categories + drill down in tenant
Enterprise-readiness score and risk rating of discovered apps	Top apps only	Summarised for all apps + drill down in tenant
App risk analysis	---	App risk breakdown overall and in key categories
Data movement analysis	Summary of data movement	Detailed summary of data movement, including by users and locations
Sanctioned app analysis	Summary of usage	Usage analysis + enterprise-readiness gaps
Usage and activity analysis[1]	Summary of risky activities	Risky activities (e.g., sharing, downloading, etc.) in key apps
Cloud usage mapped to EU GDPR	---	Cloud usage analysis against six EU GDPR focus areas for cloud-consuming organisations
Sensitive data exposure analysis (DLP violations in content at rest)[2]	Summary of DLP violations	Violations by type vs. total files scanned + exposure breakdowns
Sensitive data violation analysis (DLP violations in content en route)[3]	Summary of DLP violations	Violations discovered en route to and from discovered cloud apps
Recommendations	---	Recommendations mapped to EU GDPR + phased remediation roadmap

[1] Available if the Netskope CRA for the EU GDPR is performed in-line or in secure TAP deployment mode
[2] Must perform content discovery against DLP profile(s) as part of Introspection
[3] Available if the Netskope CRA for the EU GDPR is performed in-line or in secure TAP deployment mode with DLP profiles enabled

How to take advantage of the Netskope CRA for the EU GDPR

To take advantage of the Netskope CRA for the EU GDPR, all you need to do is upload your web proxy or firewall logs to a secure, dedicated SOC-1 and SOC-2 Type II-certified Netskope tenant instance. You may also choose to have Netskope perform the assessment using alternative deployments, including Introspection, secure TAP, or in-line, which will give you additional visibility into DLP violations and granular activity details. Once the analysis is complete, Netskope will present Netskope CRA for the EU GDPR to you and your team. If you choose to pursue the Advanced Assessment, you will have access to tenant instance for one month to perform additional analysis.

About Netskope

Netskope™ is the leading cloud access security broker (CASB). Netskope gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organisations to direct usage, protect sensitive data, and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.