netskope

Compliance Series

EU Artificial Intelligence Act (2024/1689)

Netskope Product Mapping Guide

TABLE OF CONTENTS

INTRODUCTION

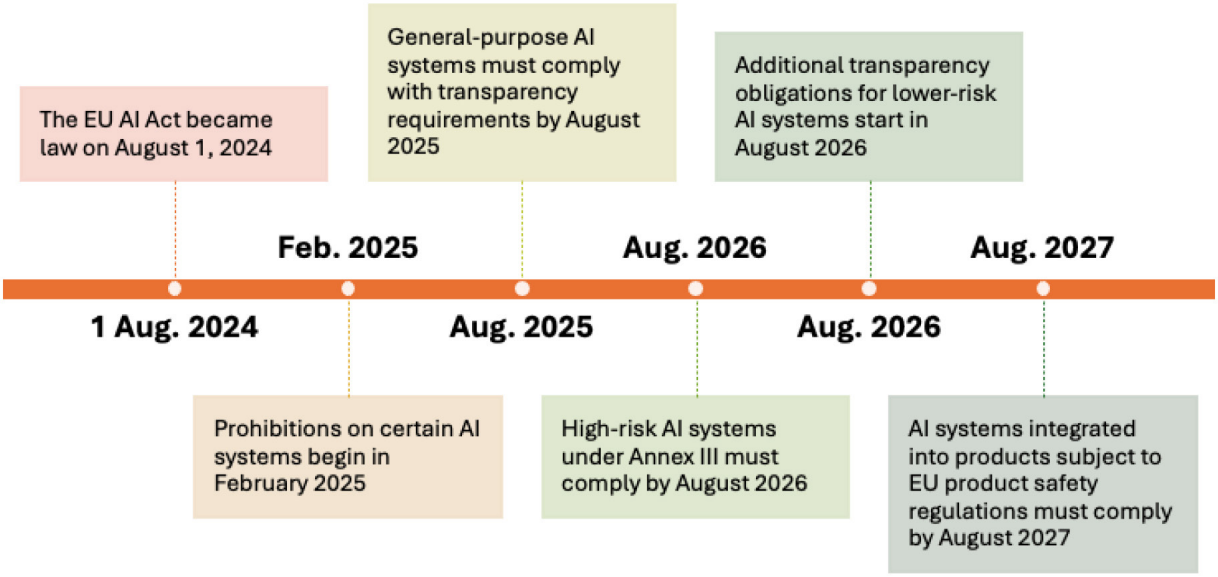
EU AI Act

The EU AI Act is a regulation enforced by the European Union aimed at governing the development, deployment, and use of artificial intelligence (AI) within the EU. It seeks to ensure that AI systems are safe, ethical, and respect fundamental rights.

The regulation classifies AI systems into four categories:

1. Prohibited: AI systems that pose a clear threat to safety, livelihoods, or rights (e.g., social scoring by governments) are banned.
2. High-Risk: AI systems that could significantly impact people's rights and safety (e.g., in healthcare, employment, law enforcement). These systems require strict compliance measures, including risk management, data governance, and human oversight.
3. General-Purpose: AI systems with specific transparency obligations (e.g., chatbots) must inform users that they are interacting with AI.
4. Minimal Risk: AI systems with minimal risk (e.g., spam filters) have no specific obligations.

Timeline



The regulation places a strong emphasis on transparency, accountability, data governance, and continuous monitoring to ensure AI systems' compliance with EU standards.

HOW TO USE THIS GUIDE

This guide has been created using the EU AI Act (2024/1689) regulation and maps Netskope's platform capabilities to the articles defined. The EU AI Act can be accessed here - https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1725546703699

As this mapping guide is based on a legal document, not all articles can be directly mapped to a technical control, such as 'definitions' and details around 'enforcement bodies'; however for the articles listed, Netskope can either partially or fully support a process or technical control including a reporting mechanism associated with the requirement.

Due to the high-level nature of the regulation, it is not possible to map each requirement to a specific product; however, a full list of Netskope's products are listed in the following table that can support many of the requirements described in the regulation.

Note the following acronyms and/or aliases for the Netskope products:

Industry terminology	Netskope Product Line/Abbreviation
Security Access Service Edge	SASE
Security Service Edge	SSE
Next-Gen Secure Web Gateway	NG-SWG
Cloud Access Security Broker	CASB
Public Cloud Security	Public Cloud Security
Zero Trust Network Access	ZTNA Next
Cloud Security Posture Management	CSPM
SaaS Security Posture Management	SSPM
Data Loss Prevention	DLP (Standard & Advanced)
Firewall as a Service	Cloud Firewall
Reporting and Analytics	Advanced Analytics
Threat Intelligence	Threat Protection (Standard & Advanced)
Remote Browser Isolation	RBI
Artificial Intelligence Security	SkopeAI
Software-Defined Wide Area Network (SD-WAN)	Borderless SD-WAN Secure SD-WAN Endpoint SD-WAN Wireless SD-WAN IoT Intelligent Accessl

Industry terminology	Netskope Product Line/Abbreviation
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

EU AI ACT MAPPING

Chapter/Article	Netskope Control & Coverage
Chapter 1 - General Provisions (Deadline Feb 2025)	
Article 1 - Subject Matter	Defines the purpose of the regulation.
Article 2 - Scope	Netskope's platform and compliance tools help organisations understand their obligations under the EU AI Act. This includes classifying AI systems according to their risk level (e.g., prohibited, high-risk or minimal risk) and understanding the roles and responsibilities defined by the Act, such as those of providers, deployers, importers, and distributors. The Netskope platform has a list of 85,000+ Cloud Service Providers (CSPs) and subcategories including providers of genAI services. This includes details of providers established and located in the EU or in a third country. Policies can be set to limit access to providers of AI services based on country, data processed, risk etc.
Article 3 - Definitions	Sets the definitions of the regulation.
Article 4 - AI literacy	The Netskope platform has a list of 85,000+ Cloud Service Providers (CSPs) and subcategories including providers of genAI services. The Netskope platform records 50+ attributes associated with each provider and can help supplement a third-party assessment review. In addition, Netskope can help identify what data is being processed by the provider and deployer of AI systems therefore assist in the consideration of persons or groups of persons on whom an AI system may be used.

Chapter/Article	Netskope Control & Coverage
Chapter 2 - Prohibited AI Practices (Deadline Feb 2025)	
Article 5 - Prohibited AI practices	The Netskope platform has inline controls that can control access to prohibited AI systems. Policies are fully configurable to also limit access to systems and monitor attempts to use approved AI systems for prohibited practices based on data that may be moved/imported into the system i.e. movement of sensitive personal data for risk assessments, profiling, movement of facial images, biometric data etc. A full list of prohibited AI systems is available with Article 5 of the regulation.
Chapter 3 - High-Risk AI Systems (Deadline Feb 2025)	
Article 6 - Classification rules for high-risk AI systems **(Deadline Aug 2027)**	The Netskope platform has inline controls that can control access to prohibited AI systems. Policies are fully configurable to also limit access to systems and monitor attempts to use approved AI systems for prohibited practices based on data that may be moved/imported into the system i.e. movement of sensitive personal data for risk assessments, profiling, movement of facial images, biometric data etc. A full list of prohibited AI systems is available with Article 5 of the regulation.
Article 7 - Amendments to Annex III	Lists High-risk AI system areas such as biometric, critical infrastructure, education etc. Netskope can assist in identifying categories of AI systems and applying controls as documented within this guide.
Article 8 - Compliance with the requirements	The Netskope platform can assist in applying classification levels to AI systems and assessing compliance with the many regulations, standards and frameworks available. The 85,000+ Cloud Service Providers (CSPs) each have a unique rating of 0-100 that can be used to help determine if an AI system is high-risk along with details of any third-party conformity assessment.
Article 9 - Risk management system	The Netskope platform can assist in continuously assessing and applying risk management principles to the lifecycle of a high-risk AI system. This can include configuring continuous assessments of the system if hosted on SaaS or Public Cloud or verifying use cases and can even identify data being processed by system and if this elevates the risk i.e. if data is being processed and includes a D.O.B of a person under the age of 18.
Article 10 - Data and data governance	The Netskope platform includes data protection capabilities to include the improvement of labelling, classifying and categorising data consumed by AI systems. In addition, data can be automatically labelled or fingerprinted to determine if its training, validation data or from a testing data set. Additional controls include limiting data if it is shared from a specific geographical location or if contextual and/or behavioural changes have taken effect through its lifecycle.

Chapter/Article	Netskope Control & Coverage
Article 11 - Technical documentation	The Netskope platform can ingest technical documentation if it's made public by the provider. This documentation may be used to supplement the Cloud Confidence Index (CCI) of 85,000 + Cloud Service Providers (CSPs)
Article 12 - Record-keeping	The Netskope platform can check if admin, user and or data access audit logs are available from the AI system provider within their service agreement. This is used to supplement the Cloud Confidence Index (CCI) score of 85,000+ Cloud Service Providers (CSPs).
Article 13 - Transparency and provision of information to deployers	The Netskope platform can verify transparency of the AI system and the details the provider makes available. This is used to supplement the Cloud Confidence Index (CCI) score of 85,000 + Cloud Service Providers (CSPs).
Article 14 - Human oversight	The Netskope platform can provide reports including activity and usage to help provide human oversight. With Netskope advanced analytics, administrators can monitor trends and identity misuse of an AI system or the data ingested or created.
Article 15 - Accuracy, robustness and cybersecurity	The Netskope platform can perform continuous assessments of the system if hosted on SaaS or Public Cloud platforms. In addition, the platform is designed to provide controls to secure access to authorised personnel, identify system vulnerabilities and prevent and/or detect attempts on data poisoning, model poisoning, model evasion through the ability to monitor input queries including confidentiality attacks or model flaws.
Article 16 - 24 Sets obligations of providers of high-risk AI systems to ensure compliance with the EU AI Act.	Netskope does not map to these articles.
Article 25 - Responsibilities along the AI value chain	The Netskope platform can assist organisations in identifying attempts to modify a high-risk AI system through continuous security assessments. In addition, the platform can also identify if the intended purpose of the AI system changes through behavioural or data specific changes i.e. data input query monitoring.
Article 26 - Obligations of deployers of high-risk AI systems	The Netskope platform can assist deployers of AI systems to apply the required technical and organisational measures. These include Data Governance and Security, Risk Management, Transparency and Accountability, Compliance Support and Human Oversight as detailed throughout this guide.
Article 27 - Fundamental rights impact assessment for high-risk AI systems	The Netskope platform can help identify the categories of natural person data used i.e. employee, customer, consumer data. Details of these categories can be provided in a report or trend analysis to provide additional context for human oversight and impact assessments.

Chapter/Article	Netskope Control & Coverage
Article 28 - 39 Sets requirements for authorities, notified bodies, obligations and conformity assessment bodies of third countries.	Netskope does not map to these articles.
Article 40 - 49 Sets standards, conformity assessment, certificate and registration	The Netskope platform can ingest public information available from providers of AI systems including if they have met the required standard for high-risk AI systems, have completed a conformity assessment, issued a certificate, declaration or received a CE marking. This data can be used to reflect the Cloud Confidence Index (CCI) score and set policy to manage access, security and compliance within the service.
Chapter 4 - Transparency obligations for providers and deployers of certain AI systems (Deadline Aug 2025)	
Article 50 - Transparency obligations for providers and deployers of certain AI systems	The Netskope platform can help identify and categorise the use of an AI system and make this information available to the user (using pop-up coaching pages) including if the service meets the requirements of forthcoming approved Code of Practices. In addition, output generated by the AI systems can be tagged, labelled and classified as machine generated if the Netskope platform has access to the repository of output data. This includes audio, image, video or text content.
Chapter 5 - General-Purpose AI models (Deadline Aug 2025)	
Article 51 - Classification of general-purpose AI models as general-purpose AI models with system risk	The Netskope platform can assist in classification of general-purpose AI models and evaluate both the AI system risk score independently and any high impact capabilities based on visibility of both data ingestion to system and data output. These classifications can be managed to coach and educate users of systems in addition to providing a reporting mechanism to identify any system risks.
Article 52 - 55 Defines procedures, obligations, representatives, and systemic risk requirements for providers	Netskope does not map to these articles.
Article 56 - Codes of Practice	The Netskope platform can assist in identifying AI systems that have aligned to an approved Code of Practice. This is subject to Codes of Practice being available for providers of services listing their alignment to a Code of Practice publicly.

Chapter/Article	Netskope Control & Coverage
Chapter 6 - Measures in support of innovation	
Article 57 - 63 Covers AI regulatory sandboxes, including testing and derogations for providers and operators. Article 59 covers use of personal data in AI regulatory sandbox	The Netskope platform can assist in identifying AI systems that are part of the AI regulatory sandbox if this information is made public including details of location and service terms. In addition, the Netskope platform can help identify and control the use of personal data in an AI regulatory sandbox for input/output as referenced in Article 59.
Chapter 7 - Governance (Deadline Aug 2025)	
Article 64 - 70 Covers the development of an AI office, AI board, Advisory forum, panel and point of contacts for the EU	Netskope does not map to these articles.
Chapter 8 - EU database for High-Risk systems (Deadline Aug 2025)	
Article 71 - EU database for high-risk AI systems listed in Annex III	The Netskope platform can assist in leveraging the EU database for high-risk systems and making this information available to a user when they are connecting to or using an AI system published in the EU database. This requirement is subject to the availability of an EU database being available by the deadline of August 2026.
Chapter 9 - Post-market monitoring, information sharing and market surveillance	
Article 72 - Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	The Netskope platform can assist in continuously evaluating AI systems including possible interaction with other AI systems. This information is available within the Cloud Confidence Index (CCI) score of 85,000 + Cloud Service Providers (CSPs) including AI system providers.
Article 73 - Reporting of serious incidents	The Netskope platform can alert when a public disclosure has been made by the provider of AI systems. Details of the incident including details of a data breach, can affect the Cloud Confidence Index (CCI) score. This information can be used to adjust access, i.e. limit access during the breach or limit what data is posted to the AI system following this notification.
Article 74 - 94 Covers enforcement from authorities including market surveillance, power of authorities, and safeguard and compliance procedures for EU	Netskope does not map to these articles.

Chapter/Article	Netskope Control & Coverage
Chapter 10 - Codes of conduct and guidelines	
Article 95 - Codes of conduct for voluntary application of specific requirements	The Netskope platform can assist in leveraging publicly disclosed codes of conduct and make this information available to a user when they are connecting to or using an AI system.
Article 96 - Guidelines from the commission on the implementation of this regulation	Netskope does not map to this article.
Chapter 11 - Delegation of power and committee procedure	
Article 97 - 98 Covers exercise of the delegation and committee procedure	Netskope does not map to this article.
Chapter 12 - Penalties (Deadline Aug 2025)	
Article 99 - 101 Covers fines and penalties for infringement of the act	Netskope does not map to this article.
Chapter 13 - Final provisions	
Article 102 - 113 Details amendment to existing regulations, directives and entry of act into force and application	Netskope does not map to this article.

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.