Managing the Challenges of the Cloud Under EU General Data Protection Regulation

netskope

Introduction

European Union data protection law requires organisations to take adequate measures to ensure the security of personal data. This obligation must be met regardless of the means used to process the personal data. The security obligation covers not only enterprise information systems, but also cloud services used to process the personal data. Data breach notification obligations, steep fines of 20 million euro or 4% of global turnover, whichever is higher, and increased public scrutiny of how organisations use and protect personal data require that they pay close attention to the security of personal data.

One of the central principles of the European Union's new General Data Protection Regulation (GDPR or regulation) is its Accountability Principle: organisations must *demonstrate* that they comply with the GDPR and that they have taken appropriate measures to ensure compliance. Add the new 'right to be forgotten' and the new privacy principles of Data Protection by Design[1] and Data Protection by Default[2] and one can conclude that managing compliance with the GDPR is going to be a challenge.

The compliance problem of unmanaged cloud services

One of the most underestimated compliance challenges that organisations face under the GDPR is the fact that many - if not most - personal data for which the organisation is legally responsible are processed in an *unstructured* way. They are not processed in pre-defined enterprise data systems or pre-approved cloud services that comply with the organisation's security policies and legal obligations, that meet the data minimisation and data quality principle, and that are regularly backed-up, patched and audited as part of the organisation's management cycle. Also, unstructured personal data are created by users – often unsupervised – using productivity or collaboration applications. These data are stored on mobile devices and shared with others through unsanctioned applications and cloud storage locations, which are outside the organisation's direct control. The trend of Bring Your Own Device (BYOD) has only exacerbated this problem.

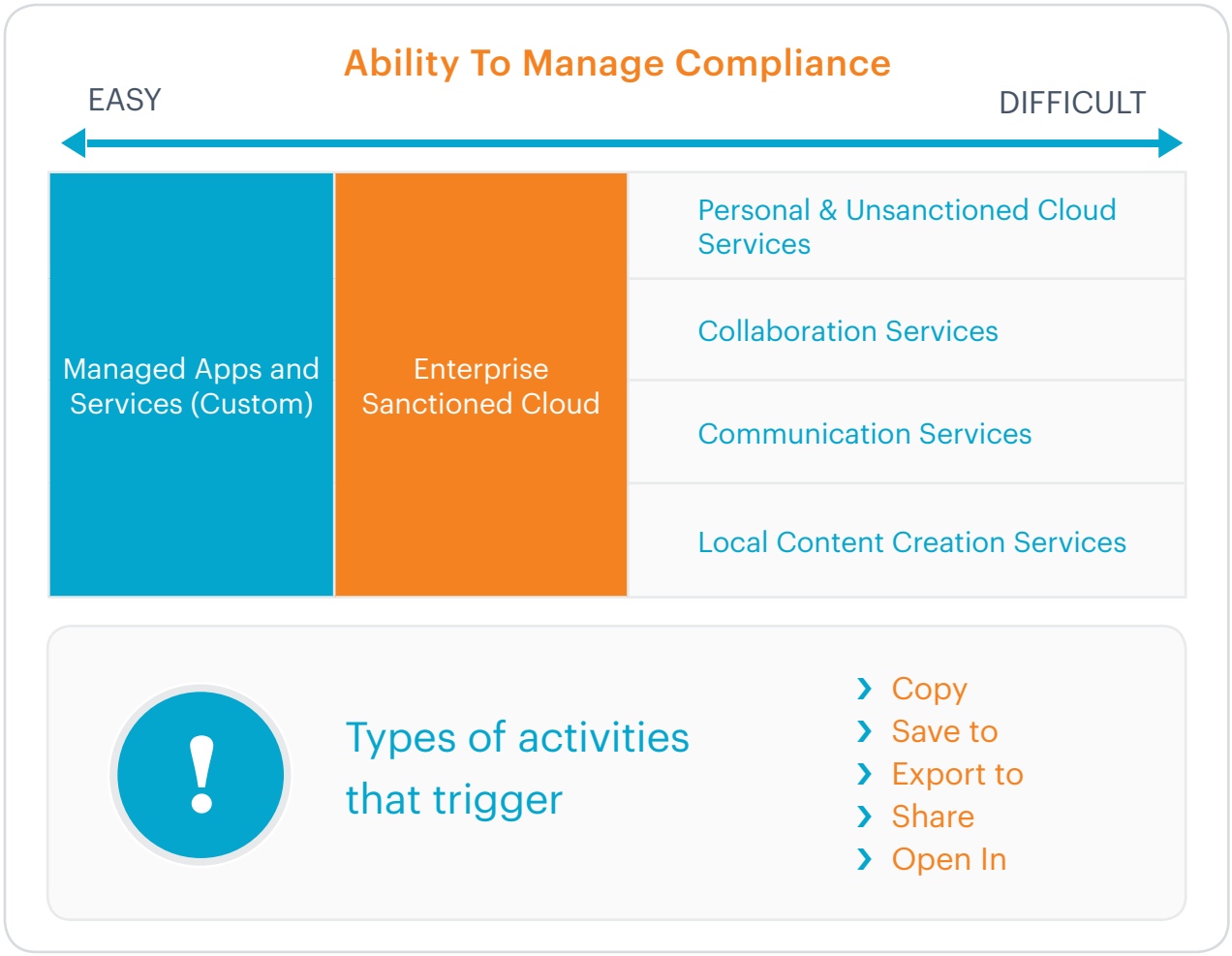
Nevertheless, under the GDPR it is always the organisation's legal responsibility to protect such unstructured data from loss, alteration or unauthorised processing, even if workers use cloud services that are not pre-approved or controlled (sanctioned) by the organisation. This means that organisations must:

- **Know** which personal data are processed by users of cloud services;
- **Identify** the cloud services and applications used by the organisation's workforce;
- **Prevent** personal data from being stored or processed in unmanaged cloud services; and
- **Protect** personal data when stored or processed in cloud services.

Failure to manage non-approved cloud services may leave the organisation at serious risk, from both a legal perspective and from a business continuity and reputational perspective. CIOs should therefore pay close attention to this issue and implement measures to bring such cloud services under the visibility and control of the organisation.

1. Data Protection by Design means that each new service or business process that makes use of personal data must take the protection of such data into consideration. An organisation needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that an IT department must take data protection and privacy into account during the whole lifecycle of the system or process development.

2. Data Protection by Default means that the strictest data protection settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user.



The General Data Protection Regulation

Under European Union (EU) law, personal data can only be gathered legally under strict conditions and for a legitimate purpose. Persons or organisations that collect and manage personal information must protect it from misuse and must respect certain rights of the data owners, which are guaranteed by EU law. The previous Data Protection Directive (95/46/EC) had caused unacceptable variety among national data protection laws, thereby creating barriers in the internal EU digital market, and did not adequately address developments in information technology, such as cloud computing and social media. Data collection had exploded, often without EU citizens consenting to the collection of their personal data.

The main goal of the EU GDPR is to protect citizens' personal data, to increase responsibility and accountability of organisations processing personal data, and to simplify the regulatory environment for business. The GDPR ensures full harmonisation of data protection law across the EU internal market; once the regulation applies, all national data protection laws will be preempted by the regulation, even if they contain stricter provisions. Furthermore, member states must bring all sectoral laws that contain data protection provisions into conformity with the regulation.

What is personal data?

Personal data is *any information relating to an individual*, whether it relates to their private, professional or public life. It can be anything from a name, a photo, an email address, a person's bank details, posts on social networking websites, medical information, work performance, subscriptions, purchases, tax number, education or competencies, location, username and password, hobbies, habits, lifestyle, or a person's computer's IP address. The GDPR applies when a person can be directly or indirectly identified by such data, or when a person can be uniquely singled out in a group of individuals.

Sensitive data

Although the GDPR does not differentiate between types of personal data based on sensitivity, some types of personal data are clearly of a more sensitive nature than others. First of all, in several places the GDPR highlights personal data of children as a type of personal data that requires extra care. The 'duty of care' argument can also be made for other categories of **vulnerable people**, such as the elderly.

Also, **data processing that poses (high) risk to the rights and freedoms of the individual** is considered extra sensitive, thus requiring data protection impact assessments to be carried out prior to the processing and notifications of data breaches to supervisory authorities and individuals. Unfortunately, the GDPR does not contain a list of personal data that would fall into the category of 'sensitive data.' However, based on the guidelines of supervisory authorities regarding data breach notification and classification of data in relation to data security, the following types of personal data should be regarded as having increased sensitivity:

- Special data (see next paragraph);
- Data relating to the financial or economic situation of an individual;
- Data that may lead to stigmatisation of or discrimination against the individual;
- Usernames, passwords, and other user credentials;
- Data which are protected by a legal or professional secrecy obligation, and
- Data that could be misused for identity fraud.

Special data

The GDPR identifies a number of personal data as 'special data.' The GDPR contains a strict **prohibition** to process such data, unless a specific exemption also mentioned in the GDPR applies, like a narrowly described use case (for example, employment law), a specific controller (for example, a non-profit organisation) or with the explicit consent of the individual. The data that fall into this category are:

- Data revealing racial or ethnic origin (for example, photos);
- Data revealing political opinions;
- Data revealing religious or philosophical beliefs;
- Data revealing trade-union membership;
- Genetic data;
- Biometrics;
- Data concerning health;
- Data concerning sex life, including sexual orientation; and
- Data related to criminal convictions, offences and related security measures.

The European right to data protection

The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, whilst receiving medical treatment, when dealing with the government or when on the Internet. This right is not only extended to EU citizens, but to all people in the world. This means that the EU not only expects governments and businesses across the world to protect the personal data of EU citizens, but also expects EU governments and businesses to protect the personal data of everyone, regardless of whether such data relates to EU citizens. Therefore, the GDPR is very extraterritorial:

It applies to

EU governments and businesses regardless whether they process personal data of EU citizens or not, as well as

non-EU businesses providing services to EU consumers or monitoring the behavior of EU citizens.

Data protection roles, rights and obligations

EU data protection law identified four roles in data protection, each with their own obligations and rights under the GDPR.

- The **controller** is the person, legal entity, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Generally, the role of the controller is derived from the organisation's **functional relation** with the individual. That is, a business is the controller for the customer data it processes in relation to its sales, and an employer is the controller for the employee data they process in connection with the employment relationship. In some cases, the role of the controller is derived from the **law or official tasks** of the organisation. For example, a tax authority is the controller for the processing of citizen's financial data in connection with taxation. Last but not least, the role of controller can be derived from the **factual influence** of an organisation over the data processing. For example, somebody who steals personal data is considered the controller for the stolen data (and lacks sufficient legal basis for the processing, making the processing illegal). A similar argument can be made for an organisation's headquarters, which requires its affiliates to process their data by using a specific cloud application.

  The controller is required to meet the obligations of the GDPR, including:

  - the requirement to have a **sufficient legal basis** for the processing of personal data (for example, consent, a contract, a legal obligation or a legitimate interest which overrides the data subject's fundamental rights, freedoms and interests);
  - the requirement to collect personal data only for specified, explicit and legitimate purposes (**purpose limitation**);
  - to limit the processing and retention of personal data to said purposes (**data minimisation**);
  - to use the data only for secondary purposes which are compatible with the purpose for which the data were collected (**use limitation**);
  - to ensure that the data are accurate, up-to-date and relevant (**data quality**),

- to take adequate measures to protect the data (**security**);
- to ensure that the personal data are processed in accordance with the principles of **data protection by design** and **data protection by default**;
- to inform the supervisory authorities and the data subject of a data breach;
- to demonstrate compliance with the GDPR (**documentation**); and
- to prevent personal data from being transferred to recipients in countries which do not provide an adequate level of protection compared to the GDPR (**data export restrictions**).

The controller is accountable for the processing of personal data and liable for any damage resulting from a violation of the GDPR rules. Where a controller processes personal data jointly with another controller, they could be jointly and severally liable towards the individual.

› The **processor** is the person, legal entity, public authority, agency or any other body which processes personal data on behalf of the controller (for example, a service provider). Typical processors are IT service providers (including hosting providers) and payroll administrators.

The processor is required to process the personal data in accordance with the controller's instructions, and take adequate measures to protect the personal data. The processor may not use the personal data for its own purposes. The processor must process the personal data in accordance with the principles of **data protection by design** and **data protection by default**, inform the controller of a data breach, demonstrate compliance with the GDPR by keeping up-to-date documentation about the processing, and prevent the personal data from being transferred to recipients in countries that do not provide an adequate level of protection. The controller is required to close a processor agreement with the processor detailing the processor's obligations.

The processor is liable for any damage resulting from not meeting its obligations under the regulation or acting contrary to the controller's lawful instructions. This includes liability for data breaches caused by the processor. It should be noted that the controller is liable for the damage caused by the processor, so controllers should do proper due diligence before engaging processors, supervise their processing of the personal data, and conduct regular audits and compliance checks to verify the processor's compliance with the regulation.

› The **data subject** is an identified individual or an individual who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other individual or legal entity. The GDPR extends specific rights to data subjects regarding the use of their personal data, such as the right to be informed about the data processing, the right to consent to the processing of their personal data (**opt-in**) or object to the processing of their personal data (**opt-out**), the right to obtain their personal data in a structured and commonly used format in order to transfer those data, in certain circumstances, to another controller (**data portability**), the right not to be subjected to fully automated data processing or profiling, the right to ask the controller whether personal data are processed about their, the right to know which data are processed (**right of access**), the right to correct where the data are incorrect, the right to complete the personal data where the personal data are insufficient in relation to the purposes for which they are processed, and the right to have the data erased under certain circumstances, for example, where the retention period has lapsed or where consent for the processing has been withdrawn (**right to be forgotten**). Furthermore, the data subject has the right to register a complaint with the supervisory authority and receive compensation for damages incurred as a result of non- compliance by the controller or processor.

- The **supervisory authority** (Data Protection Authority or DPA) is the public authority that supervises and enforces the GDPR on the territory of its Member State. Each DPA has broad enforcement powers, including the power to issues fines of 20 million euro or 4% of global turnover, whichever is higher, in cases where the data subject's rights have been infringed and 10 million euro or 2% of global turnover, whichever is higher, in cases where data controllers or processors have not met the obligations of the regulation, and the power to conduct investigations and deal with complaints. Controllers must notify the relevant DPA(s) of data breaches and certain types of processing, such as some international data transfers, require a DPA's authorisation.

The GDPR in relation to cloud services

The rules of the GDPR apply regardless of the means used to process the personal data. They apply to personal data stored on local servers, as well as on servers in the cloud. However, the cloud poses a number of specific compliance challenges to entities covered by the GDPR:

- The GDPR requires that controllers and processors **know the location** where the personal data are stored or otherwise processed. The GDPR severely limits the ability of entities covered by the GDPR to transfer the personal data to recipients outside the European Economic Area (EEA, as in the Member States of the EU, plus Norway, Iceland and Liechtenstein). Cloud services may use servers outside the EEA unknown to the controller or processor, or the cloud service's data processing equipment in European territory may be remotely serviced by non-EU service providers. In all such cases the transfer of personal data must comply with the data transfer rules of the GDPR.
- The GDPR requires that controllers **take adequate security measures** to protect the personal data from loss, alteration or unauthorised processing. The controller should **assess** whether the security measures of the processor meet the security requirements applicable to the personal data (on the basis of a risk analysis) and to the controller (on the basis of specific sectoral, contractual or organisational requirements) and must supervise the implementation of security measures by the processor by conducting regular audits. The same obligations apply to the processor using a sub-processor. However, most cloud providers do not allow their clients to provide instructions relating to data security or to conduct security audits.

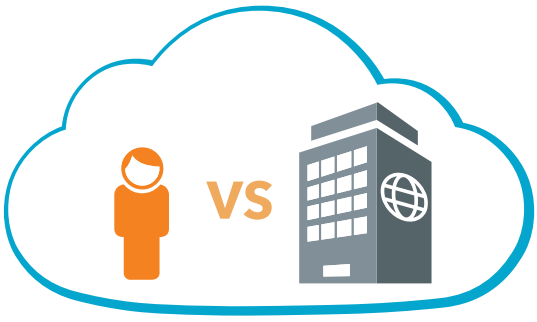
- The GDPR requires the controller to **close a 'data processing agreement'** with the processor. Such a contract must stipulate a number of particular obligations on the part of the processor, such as:
  - to act only on the instructions of the controller;
  - to take adequate security measures to protect the data from loss, alteration or unauthorised processing;
  - to engage a sub-processor only with the prior permission of the controller;
  - to assist the controller if necessary in response to requests for exercising data subjects' rights;
  - to assist the controller in meeting his obligation of notifying the supervisory authority and the data subjects of a data breach;
  - to assist the controller in conducting a 'data protection impact assessment' to identify the privacy and security risks of the processing of the personal data; and
  - to hand over all personal data after the end of the processing or the termination of the service agreement.

  However, most cloud providers provide their services on the basis of terms and conditions which do not meet these requirements and which are not or are only marginally negotiable.

- The GDPR requires that personal data are **collected only as necessary to the purpose, puts limits on the processing of special data** (such as data revealing race, ethnic origin, biometrics, political conviction, religious or philosophical beliefs, data concerning health and sex life, union membership, and data relating to criminal convictions or offences) and **puts limits on the processing of certain sensitive data**, such as tax numbers and data relating to children. This requires a detailed assessment of the functionality and data elements of applications *before* they are put to use. Many cloud services only unveil their full functionality and data requirements *after* organizations have started to use them.
- The GDPR does **not allow data processors to use the personal data for other purposes** beyond providing the services to their customers. However, many cloud services reserve the right to use the data for all kinds of secondary purposes, such as marketing. Especially when cloud services are offered for free, cloud providers use the data in some way to generate revenues. Some cloud providers even claim full ownership of the data stored in their environment and sell the data to third parties.
- The GDPR requires personal data to be **erased when the purposes of use have ceased to exist.** This means that organisations must specify data retention limits for the data (in advance), have the data automatically erased from their systems or organise for the data user to take an informed decision on the further retention of the data, and conduct audits to check whether the data have actually been erased. Many cloud services are not clear about their data erasure procedures or tell their users to erase data, so the organisation may be in breach of the regulation because the data are not properly erased from the cloud services.

Personal cloud services and BYOD

While responsible organisations will try to minimise the risks posed by cloud services by selecting reputable vendors, performing security risk assessments and compliance checks, and closing processor agreements or agreeing with terms and conditions that meet the GDPR requirements and company policies, workers often do not think of such risks when using personal cloud services not authorised by the organisation, let alone take steps to minimise such risks.



The possibility to connect personal devices such as laptops, tablets and smartphones to the organisation's network ('bring your own device,' or BYOD) has further increased the risk of non-compliance with the GDPR. Many consumer devices are sold with free cloud services pre-installed on them. Furthermore, some users download risky software onto their devices. This means that organisations put personal data at risk when they do not take steps to prevent those data from being automatically uploaded to a user's personal cloud or other cloud applications, sometimes even without the user being aware of this. The organisation is often not in a position to exercise control over such services and applications, and has to rely on the worker acting responsibly when accessing and storing personal data from the company's network on his or her personal device and on the default settings of the device and the applications.

Not knowing where the personal data are stored, how the personal data are protected, which personal data are created, collected and used for what purposes, how long the data are retained and who has access to the data exposes the organisation to investigations, fines and negative publicity associated with data breaches or exposures. Therefore, organisations should do their utmost to block or limit the use of unmanaged cloud services, or put rules around the use of such cloud services.

How can Netskope help organisations manage their GDPR risks?

The complexity of their landscape, including the use of cloud services, requires organisations actively to take measures to protect their personal data. Because of this complexity and because of the vast amount of data processed, it no longer suffices to comply with the GDPR only through legal arrangements like policies, protocols and contracts. Your organisation must be sure personal data are processed in ways consistent with the GDPR. This means that you must take organisational and technical measures, beyond traditional security measures that are aimed at confidentiality, integrity and availability of the data, in order to ensure compliance with the GDPR (data protection by design).

One type of measure that you can take to manage your compliance with the GDPR is to control your organisation's interactions with the cloud. You do this by:

- **Knowing** which personal data are processed by workers using cloud services;
- **Identifying** the cloud applications used by your workforce;
- **Preventing** personal data from being stored or processed in unmanaged cloud services; and
- **Protecting** personal data when stored or processed in cloud services.

Failure to meet these requirements may leave your organisation vulnerable to fines, lawsuits and negative publicity because of GDPR violations.

Know what personal data are processed by cloud services

Privacy compliance starts with knowing which personal data are being processed in your organisation. 'Data mapping,' the exercise of identifying personal data in the organisation and mapping them to (legitimate) purposes, is relatively easy for personal data stored in enterprise information systems. With cloud services, and especially with unmanaged and unsanctioned cloud services, knowing which personal data are being processed is much harder. Many cloud services allow for far more data to be processed than is necessary or allowed, and the data flows to and from the cloud are almost invisible to the people in the organisation responsible for GDPR compliance.

This means you need a tool to help you identify the personal data being uploaded to or downloaded from the cloud. This applies not only at the perimeter, but right up to the level of the individual worker, so you are able to discuss and understand the need and the purposes for such personal data as well as their use by your organisation. Netskope allows you to set policies around specific types of personal data. For instance, you may block the upload or download of certain types of personal data to cloud services, such as employee photos, social security numbers, customer credit card information or health information. Knowing this type of data is processed via the cloud enables you to assess such processing and to make informed decisions as to the lawfulness and necessity of such data, mitigate your cloud related privacy risks and assess your organisation's overall compliance with the GDPR.

The Netskope Active Platform™ allows you to drill down into activity- and data-level usage details of cloud apps. This allows you to answer questions like "Are any unauthorised users downloading personal data from any of our human resources apps?" or "What sensitive content do we have in our sanctioned cloud storage service?" You are also able to see who shares personal data with recipients outside of the organisation using cloud email, a cloud storage or file-sharing service or other data sharing, assess whether the disclosures are allowed under the law and your privacy policies, and if necessary, set policies to ensure that certain personal data cannot be shared with people outside of the organisation. Audit trails allow you to follow suspicious events.

Identify the cloud services used in the organisation

Knowing which personal data are being processed in the cloud and for which purposes is only the first step. The next step you must take to achieve compliance with the GDPR is to understand which cloud services are being used, the terms and conditions as well as the policies of such cloud services, especially regarding the use, security, disclosure and retention of personal data, and the locations of the servers where personal data will be hosted.

With the Netskope Cloud Confidence Index, you are able to assess both your managed and unmanaged cloud services on their suitability to host enterprise data, including personal data for which your organisation is responsible. The Netskope Cloud Confidence Index uses more than 40 parameters adapted from the Cloud Security Alliance's Cloud Controls Matrix, including a cloud service's security features (for example, whether data are encrypted at rest), data classification capabilities, certifications (for example, ISO27001, SOC-2 or TRUSTe's Trusted Cloud Privacy Certification), and whether the service enables audit logging to see unauthorised access or activities.

Furthermore, Netskope allows you to identify cloud services that do not meet the standards for data ownership (with a specific GDPR readiness rating), because – according to their terms and conditions – they take ownership of the data once the data are uploaded to the cloud environment. It also allows you to identify services that do not meet your privacy standards by showing you whether they allow third-party cookies, access personal data stored on a device, access other services on a device, or have a data retention policy that doesn't meet your needs (identifying whether they delete data within the first week, month, or not at all upon service termination). Netskope allows you to enforce policies based on this information, for example, blocking cloud services or activities within those services (such as upload) that don't meet your privacy thresholds, thus making it impossible for workers to upload your organisation's personal data to their unsanctioned and possibly unsafe clouds. Netskope even allows you to redirect personal data that workers try to upload to their unsanctioned cloud apps to enterprise-sanctioned cloud environments, or quarantine it for review, such as by a legal professional. It distinguishes between a corporate version of a cloud service and a user's private version of the same service (for example, a corporate-sanctioned instance of Box vs. a user's private instance). And it allows you to identify personal devices being used to access your cloud services, so you can enforce policies on mobile devices to ensure that corporate data are not backed up to mobile apps like iCloud. This way, Netskope helps you to meet your GDPR obligations related to disclosure of data to third parties and meet the principles of data minimisation, data security and privacy by design.

In order to comply with the GDPR's data export rules, Netskope allows you to identify the jurisdictions from which the data are uploaded as well as to identify the jurisdictions where the servers are located, even if only temporarily. This enables you to prevent personal data from being transferred to jurisdictions that do not provide an adequate level of protection to personal data as required by the GDPR.

Prevent personal data from being processed in unsanctioned cloud services

Once you have identified the personal data in your cloud services and which services process such data, you should ensure that services that do not meet the GDPR's privacy standards are not used by your workforce. This applies both to enterprise cloud services, which may be fine for use in non-EU jurisdictions but not in the EU, as well as users' private apps and services.

Netskope Cloud DLP allows you to block the upload of special personal data, such as health information or photos, as well as other sensitive personal data that your organisation chooses to protect, such as credit card information, customer email addresses or personnel records, using a specific pre-defined GDPR profile (or a customized one can be created). Sensitive data can be obfuscated, so your IT personnel cannot see the content of the file that is uploaded to the cloud, but only knows that such file contains sensitive data that shouldn't be uploaded to that particular cloud service. The DLP dashboard also allows you to identify a user who tries to upload the sensitive personal data to the cloud, as well as the source and the destination of the data. Until a violation occurs a user's name can be obfuscated as well.

Another important feature is Netskope's ability to identify users who have had their credentials compromised in another breach. This allows you to alert users to reset their passwords, and even allows you to initiate a workflow to reset the user's credentials within single sign-on (SSO) across all enterprise-managed apps.

This allows you to prevent personal data breaches, investigate incidents and report them as required, as well as to take measures (including disciplinary measures) to prevent such incidents from happening again.

Protect personal data when using cloud services

To the extent that your organisation allows certain cloud services to be used, the GDPR requires you to take adequate protection measures to protect personal data from unauthorised access. It is not sufficient to rely on the cloud app's security measures, over which you have no control. The GDPR requires you to take measures to protect the data yourself, or supervise the way a service provider (processor) protects your data. And since cloud services typically do not allow you to supervise security, you need to take measures to protect personal data before they are transferred to the cloud.

Netskope allows you to encrypt all personal data before they are uploaded to the cloud, so the data are encrypted en route to and at rest in the cloud. Encryption can also be used as an alternative to the erasure of the data. In such cases, the data are encrypted and keys are deleted. The data can also be quarantined for further inspection before being uploaded to the cloud. You may also send an automated alert to the user to let him or her know that he or she is attempting to process personal data in a way inconsistent with your organisation's privacy policy. Where personal data already have been uploaded to a sanctioned cloud service, Netskope's introspection capabilities allow you to inspect data retroactively, regardless of when the data were uploaded, and encrypt such data or restrict sharing. Netskope has API-level integration with various partners including Google, Microsoft, Box, Dropbox, Salesforce and Egnyte that allow such retroactive inspection. With the API-level integration, malware scans and remediation can also be completed to ensure the organisation is protecting data from being compromised. For unsanctioned cloud services, malware scanning can be achieved through inline deployments to scan real-time activities like uploads and downloads.

Running Netskope under the GDPR

As Netskope generates personal data itself (for example, identifying a user in an audit or DLP report), your use of Netskope must also comply with the GDPR, if:

1. Your organisation is established in a Member State of the European Union or in Norway, Iceland or Liechtenstein (as in the European Economic Area); or
2. Your organisation is not established in the European Economic Area, but you use Netskope to monitor the use of cloud services by staff located in the European Economic Area.

The two most important issues related to your use of Netskope under the GDPR are:

- Employee privacy; and
- Compliance

Employee Privacy

As Netskope utilises drill-down reports of cloud data all the way to the user level, the Netskope solution can be qualified as an 'employee monitoring system,' even when the personal information is encrypted or obfuscated by Netskope. Netskope allows tenant admins to view unencrypted audit data (events, alerts, quarantine, and legal hold), reports, and data on an app's top users. Therefore, organisations that are planning to use Netskope to protect their personal data and to enhance their compliance with the GDPR must also pay attention to the issue of employee privacy under the GDPR.

The GDPR allows EU Member States to adopt national legislation to protect employee privacy, provided such legislation is in line with the GDPR. This means that organisations planning to use Netskope must carefully identify the relevant jurisdictions where Netskope is used and their specific GDPR and national obligations related to employee monitoring. Such obligations may include:

- Establishing a legal basis for the monitoring of employee use of cloud services;
- The obligation to inform the employees about the purposes of Netskope and its general features;
- The obligation to inform employee representatives or works councils of the use of Netskope and where required obtain their consent;
- The obligation to perform a data protection impact assessment on Netskope, and to document the use and retention of its reports and the procedures allowing the employees to exercise their privacy rights under the GDPR.

Legal basis

Without any national requirement specifying the legal basis for monitoring of employees, the use of Netskope may most likely be based on the legitimate interest of the organisation to protect personal data stored in cloud environments. The GDPR has specific rules for processing personal data on the basis of a legitimate interest, such as the requirement to inform the employees of the reasons why the legitimate interest of the organisation overrides the privacy interests of the employees.

Information to employees

The organisation must inform its employees about the use of Netskope prior to the employee being monitored. Typically, the information is provided via a privacy notice to the employee, for example, by sending an email to the employee's email address or via other suitable means, such as terms of use of the organisation's network at logon.

Works councils

Many EU Member States have laws giving works councils or employee representatives consultation or co-decision rights related to employee privacy or employee monitoring. Where such laws exist, organisations using Netskope must comply with such laws, and inform their works councils about the use of Netskope and where required obtain their consent. Often, the works council agrees to the use of an employee monitoring system by agreeing to a privacy policy related to such system, so one should consider drafting a privacy policy for the use of Netskope.

Data protection impact assessments and documentation

The GDPR requires organisations to perform data protection impact assessments when the data processing likely poses high risk to the personal data. Given the fact that this requirement will most likely be further detailed by the national supervisory authorities, we cannot say for sure whether a data protection assessment for the use of Netskope is required or not. Furthermore, it is possible that national law may require data protection impact assessments to be carried out for employee monitoring systems.

The GDPR requires organisations to document their data processing in order to demonstrate their compliance with the GDPR. This requirement may also apply to the use of Netskope.

Compliance

Netskope's data centers are located on the east and west coast of the United States, Amsterdam (The Netherlands) and Frankfurt (Germany) as well as in Singapore and Sydney. Compliance with the international data transfer rules of the GDPR can be achieved by having reports relating to EU affiliates stored in Netskope's data centers in Amsterdam or Frankfurt. However, if your organisation is located in a country outside the European Economic Area, your access to the data stored in Netskope's data center must be covered by a data transfer mechanism between the data center and you, that complies with the data transfer rules of the GDPR.

If your organisation is not established in the European Economic Area and you monitor the cloud use of people located in the EU by running Netskope in a non-EU data center (US, Singapore or Sydney), you still have to comply with the GDPR. In such case, the data transfer rules of the GDPR do not apply to your personal data, because there is no international data transfer within the meaning of the GDPR. However, you must appoint a representative in the EU, who acts as a contact for the EU individuals whose cloud use is being monitored.

Netskope and GDPR at a glance

GDPR PRIVACY REGULATORY PRINCIPLES	HOW NETSKOPE HELPS WITH GDPR CLOUD-READINESS
Controllers and processors **know the location** where personal data are stored or otherwise processed	› Use Netskope to assess where data are stored and/or processed for each processor (cloud service). › Enforce policies with the Netskope Active Platform for processors that do not store/transfer data in secure locations (on List of Adequate Jurisdictions maintained by the European Commission of approved countries and territories) or process data in undetermined locations, such as blocking cloud service from being used. › Run reports on application/service usage summarized by destination location.
Controllers **take adequate security measures** to protect personal data from loss, alteration, or unauthorised processing.	› eDiscover and protect sensitive data at rest in a sanctioned processor (cloud service) or for real-time activities in all cloud services using Netskope Cloud DLP with support for 3000+ data identifiers, 500+ file types, language-agnostic double-byte characters, custom regular expressions, proximity analysis, fingerprinting, and exact match, and more. For example, use the Netskope pre-defined GDPR DLP profile (or use a custom one) to find PII and encrypt it or quarantine it and pull it back on-premises (or put in legal hold for review) as processors and controllers are required to notify users if their unencrypted personal data have been lost and must notify supervisory authorities of a data breach. › Apply security policies such as "Block use of cloud storage services rated 'Medium' or below from use" to ensure organizational usage of secure, vetted processors only. › Detect and automatically remediate cloud threats and malware like ransomware resident in sanctioned services or in real-time activities like uploads and downloads to prevent information from being stolen. › Identify credentials compromised in another breach and correlate activity within processors contracted by controller, to initiate a workflow to reset credential within SSO across all enterprise-managed (sanctioned) processors.
Controllers **prevent** personal data from being uploaded to personal cloud services and personal devices (BYOD) or **enforce** the organisation's security measures in personal clouds and devices.	› Understand and query on all access and activities by device and device classification, for example, BYOD. › Enforce access and activity-level policies based on device type and classification. › Enforce policies on mobile devices to ensure that corporate and personal data are not backed up to mobile apps or using mobile apps to back up data to cloud. Integrate with MDM solutions for additional device-level control. › Enforce policies to ensure that corporate and personal data only go into processors approved by company and not personal instances on the same processor, for example, allow upload of confidential data to corporate Box but not to personal instances of Box. › Differentiate between processor (service) instances to ensure corporate policies and visibility only in place for sanctioned processors and personal data related to organisational and business processes.
Controllers **know the privacy and security standards** the processor adheres to and **assess** those standards	› Track personal data with cloud forensic analysis to log and audit which processors have processed and/or possess personal data to comply with requests for information on individual's personal data. › Assess enterprise-readiness of processors on 40+ parameters with CCI (including privacy features such as whether app enables sub-processors or does anything else with data as well as data security features such as encryption of data at rest and cipher type). Netskope also determines GDPR-readiness of apps on a high, medium, low scale based on the parameters. › Use CCI to see if processor enables audit logging to determine whether unauthorised individuals access cloud service. › Use CCI to determine physical and logical security measures of processor, such as SOC-2 and ISO27001, not to mention app privacy seals such as TRUSTe and compliance certifications like Privacy Shield.

Controllers close a **'data processing agreement'** with processors	› Find processors (specifically those that deal with personal data) in use throughout organisation with Netskope Discovery to decide which to sanction (close agreement with) and which to restrict. › Use CCI for procurement information of processor including pricing, user models, etc.
Personal data are **collected only as necessary to the purpose of use with limitations on processing of 'special data' and 'sensitive data'**	› Restrict upload or download of "special data" and "sensitive data" per definition with Netskope Cloud DLP. › Assess functionality and data elements of processor before it is put in place for the organisation using CCI.
Processors do not use personal data for any other purposes beyond providing services to their customers	› Using CCI, run reports on which processors do not adhere to standards for data ownership (that is, specify that the vendor and not the customer owns the data) as well as privacy controls (that is, whether they allow third-party cookies, access of personal data on the device, and access of other apps on the device), including whether personal data are used for such things as marketing purposes, etc.
Personal data are to be **erased when the purpose of use have ceased to exist**	› Show which processors do not erase data or erase it right away (Netskope shows this by first week, first month, or at all). › Encrypt data at rest as an alternative to data erasure (encrypt all data or all sensitive data and then delete the encryption keys) after termination of services with processors.