netskope

EU GDPR Cloud-Readiness & Compliance Checklist

GDPR AND CLOUD SERVICES

The new set of European Union laws regarding personal data security in organisations, the **EU General Data Protection Regulation (GDPR)**, is set to be finalised and requires organisations be compliant by 2018. As organisations start taking action to comply with the GDPR within the deadline, one of the most difficult areas is the cloud.

One of the biggest problems that arises with the cloud is that personal data are processed in the cloud, with IT and security teams having no visibility or control into what is happening with the data. Employees are using unsanctioned, and possibly risky, cloud apps and services to get their jobs done. The trend of bring-your-own-device (BYOD) has only made the problem worse, with personal devices accessing personal data and syncing them outside the organisation, or worse still, using them for purposes other than those that the service purports to cover. Regardless, organisations are still on the hook for protecting personal data under the GDPR.

So how should security teams secure cloud app usage without blocking everything and inhibiting employee productivity? Working with European data privacy compliance legal expert, Jeroen Terstegge, at Privacy Management Partners, we've created a white paper on the GDPR regulations, grouping them under six encompassing principles for the cloud with an extra consideration for BYOD. As you will see below, processors (the term used in the GDPR text) are the cloud apps and services. In this checklist, we have mapped a list of actions for organisations and processors back to each principle in order to help your organisation to be cloud-ready, secure, and compliant with the GDPR.

CHECKLIST FOR GDPR CLOUD COMPLIANCE

General items for compliance with the GDPR:

- ✓ Ensure you have explicit consent from the data subject for personal data that have been collected
- ✓ Document and create data security processes (for example, data integrity monitoring, backups, etc.), auditing, and procedures such as a process of notifications to appropriate stakeholders in case of a data breach, without delay and within the required timeframe
- ✓ Request documentation from partners and vendors on their data security processes and procedures to demonstrate compliance and have an audit trail
- ✓ Appoint an independent Data Protection Officer (DPO) proficient in IT processes, data security, and privacy regulations if your company has over 250 employees or your main activity is focused on processing
- ✓ Prepare for and implement Data Protection Assessments
- ✓ Train security personnel in your organisation on the GDPR and the new rules and regulations either through manuals or by contracting outside experts
- ✓ Ensure the organisation is able to exercise data subject rights, including their right to be forgotten, right to request a copy of their personal data in a usable format, etc.
- ✓ Guarantee data security is part of the product development process to abide by Privacy by Design and Default codes in GDPR

SIX CLOUD CONSIDERATIONS FOR GDPR COMPLIANCE

1. Controllers and processors **know the location** where the personal data are stored or otherwise processed.

Controllers and processors must know where personal data are located and processed. This will enable better compliance with requests for information on individuals' personal data and requests to track locations and how the data are being used.

✔ Assess where data are stored/processed for each processor (cloud service)
✔ Determine which processors do not adhere to standards for data ownership, privacy, and data protection/security, which can lead to data being processed outside of known locations
✔ Enforce policies on processors that do not store/transfer data in secure locations on the list maintained by the European Commission of approved countries and territories, or that process data in undetermined locations
✔ Track personal data with cloud forensic analysis to log and audit where and how personal data have been used

2. Controllers **take adequate security measures** to protect personal data from loss, alteration, or unauthorised processing. Controllers will also **assess** whether the security measures of the processor meet the security requirements applicable to the personal data.

Controllers and processors are required to notify users if unencrypted personal data have been lost, and must notify the proper DPA as well. Organisations will need to investigate processors to ensure that they are protecting data appropriately and with the correct security measures and have insurances such as privacy seals (for example, TRUSTe). Ensure that you can audit your processors to prove you are doing everything within your power to protect personal data.

✔ Assess enterprise-readiness of processors on a comprehensive set of security and privacy parameters, including data security features like encryption of data at rest, cipher type, if audit logging is enabled, and physical and logical security measures such as SOC-2 and ISO27001
✔ eDiscover and encrypt/protect sensitive information in sanctioned processors - for example, find personally identifiable information (PII) and encrypt it or quarantine it and pull it back on-premises, or put in legal hold for review
✔ Apply real-time security policies such as "Block use of unapproved cloud storage apps" or "Block use of cloud storage apps rated 'Medium' or below from use" to ensure organisational usage of secure, vetted processors only
✔ Use real-time cloud data loss prevention (DLP) to identify personal data and block (or apply policy) en route to or from processors
✔ Integrate cloud security controls with a single sign-on (SSO) vendor to further secure sanctioned app usage
✔ Identify users with compromised credentials in another breach and initiate a workflow to reset credentials within SSO across all enterprise-managed (sanctioned) processors

3. Controllers **close a 'data processing agreement'** with processors.

The GDPR create an opportunity to decide on which cloud services to sanction and standardise on, as well as an opportunity to improve vendor assurance and procurement processes and make sure requirements are introduced to comply with the GDPR. You will also want to make sure processors are not engaging with sub-processors without your permission and that there is a process for auditing and assessing security of processors.

✔ Find processors in use throughout the organisation to decide which to sanction and monitor, in which to control usage, and which to restrict
✔ eDiscover and protect (e.g. encrypt) sensitive data, whether en route to or from processors or at rest in sanctioned cloud apps

4. Personal data are **collected only as necessary to the purpose of use with limitations on processing of ‘special data’ (data of vulnerable people such as the elderly) and ‘sensitive data’ (data concerning race, political opinions, religion, trade-union membership, genetics, health, sex life including sexual orientation, and criminal convictions and offences).**

Collection of personal data are only as needed under the GDPR. To increase privacy, you can encrypt data being uploaded to cloud apps or already resident in sanctioned apps.

- ✔ Restrict upload or download of “special data” and sensitive data with cloud data loss prevention
- ✔ Assess the functionality of the processor before is it put in place for the organisation to use
- ✔ eDiscover and protect (e.g. encrypt) sensitive data, whether en route to or from processors or at rest in sanctioned cloud apps

5. **Processors don’t use personal data for any other purposes** beyond providing services to their customers.

Some processors, per their operating agreements and usage terms, own the data uploaded into the system and may use the data for purposes such as marketing. You will need to ensure that personal data are being used for only what is necessary and that the processor does not own the data. While Netskope cannot guarantee that your processors are not using the data for other purposes, our Cloud Confidence Index (CCI) data and reports can give you a sense of whom to ask, where to look, and what the public stance of the processor is with regard to the data.

- ✔ Identify which cloud apps are in use that do not specify whether the vendor or customer owns the data
- ✔ Remediate through either a processing agreement or by blocking access, upload of data, or upload of certain kinds of data to such apps

6. Personal data are to be **erased when the purpose of use has ceased to exist.**

Processors and controllers are required to erase personal data when services are terminated and the personal data are no longer needed. Many processors do not erase data right away – one way to counteract this is to encrypt all data and delete the encryption keys.

- ✔ Identify which cloud apps are in use that do not erase data in a timely manner after the service has been discontinued
- ✔ Remediate through either a processing agreement or by blocking access, upload of data, or upload of certain kinds of data to such apps
- ✔ As an alternative to trusting the vendor’s data erasure policy, consider encrypting content containing privacy data using your corporate key manager, and delete the encryption keys after the service has been discontinued

ADDITIONAL CONSIDERATION: PERSONAL CLOUD SERVICES AND BYOD

Unfettered access to cloud services across mobile and bring your own device (BYOD) may present risks as many mobile devices automatically back up data to the cloud. Besides this, when it comes to personal devices, you need to be able to ensure personal data are not used improperly (whether on purpose or not).

- ✔ Query for and understand all access and activities by device & device classification, for example, BYOD
- ✔ Enforce access- and activity-level policies based on device type and classification (such as that of corporate-owned devices)
- ✔ Integrate with MDM providers to provide additional security and controls over company-issued devices and help with inventory and management of corporate assets
- ✔ Enforce policies to ensure that corporate and personal data only go into processors approved by the 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 (app) instances to ensure corporate policies and visibility instituted only for sanctioned processors and personal data related to organisational and business processes

CONFIGURE YOUR CLOUD ACCESS SECURITY BROKER (CASB) TO ENSURE GDPR CLOUD READINESS

To achieve GDPR cloud compliance, we recommend that you implement a Cloud Access Security Broker (CASB) solution such as Netskope for your organisation. However, as CASBs can also be deployed as cloud services, they must comply with the same rules and regulations. Below is a list of actions to take when implementing a CASB vendor to ensure that you are both cloud ready for the GDPR and enabling your employees to embrace the cloud.

- ✓ Assess your CASB vendor based on same GDPR principles as above
- ✓ Consider using a CASB that offers an on-premises, secure appliance
- ✓ Ensure that your CASB gives you the ability to obfuscate privacy data
- ✓ Ensure that your CASB enables role-based access to obfuscated data, and supports your legal and HR policies for viewing those data
- ✓ Ensure that your CASB has the appropriate security certifications such as SOC-1 and SOC-2 Types I and II
- ✓ Obtain user consent before you begin monitoring cloud activity
- ✓ Establish legal basis and business case for CASB implementation (possible to use GDPR as reference to track and secure personal data flow)
- ✓ Document all use and retention of reports and procedures with CASB and personal data tracking
- ✓ Ensure appropriate processes are in place for employees to exercise privacy rights under the GDPR

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.