Nextcloud

GDPR Overview

12 steps to GDPR compliance

General Data Protection Regulation

Compliance Kit

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

12 steps to GDPR compliance

On the 25th of May 2018 the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) will become enforceable. This regulation intends to strengthen and unify data protection for all individuals within the European Union (EU), but applies to any entities processing the personal data of EU citizens.

The law creates complications for organizations dealing with data of private citizens, especially when it is being shared across organizational boundaries. Compliance is simplified when data stays on premises, which is why self hosting with Nextcloud is among the easiest ways of ensuring compliance with the GDPR and similar laws across the globe.

Goals of this document
In this document, we aim you a basic overview of the steps that should be taken by any organization in order to be GDPR compliant. See the Nextcloud GDPR Admin Manual for specific details on how to comply with GDPR requirements like data export and deletion in Nextcloud.

Also please be aware that **this is in no way legal advice**. If you are unsure about GDPR compliance in Nextcloud, please get in touch with us through gdpr@nextcloud.com or contact a legal expert!

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

1/ Be aware of the changes you will need to make

First of all, you should **identify the areas in your organization that could cause compliance problems**. One way to do that is, if you have one, to consult your risk register.
If your organization is large, don't forget: Being compliant takes time and energy, which you shouldn't underestimate. By now, you should already have taken the 12 steps described in this guide - if you haven't, get started now, and consider this an urgent task! **You need to be compliant by May 25th, 2018.** A delay in completing these key steps means you will not be compliant on time and risk a fine, going up to €20 million, or 4% annual global turnover of your organization or company – whichever is higher.
Also, you should make sure **all key personnel in your organization is aware of the law changes that come with the GDPR** in order to make sure no decision which could break the GDPR law gets taken inside your organization while becoming compliant or while making future changes in the way your organization deals with data.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

2/ Become aware of the information you hold

In this second step, it is essential to **document which personal data of your staff or users you hold**. You will not be able to be compliant if you are not aware of which information you hold, and the GDPR requires you to document, demonstrate and record in which way your organization is compliant.

Here are the **questions you should ask yourself when documenting**:
- Why are you holding data?
- Why did you gather the data?
- How did you obtain the data?
- How long will you store the data?
- How securely are you storing the data? How is it encrypted? Who can access it?
- Do you share this data with third parties? On what basis are you sharing the data with those third parties?

While it is possible to achieve this goal in a rather simple way for small organizations, if your organization is a large one, you may need an **information audit** in order to get enough knowledge about the data you hold.

Documenting gets even more important if your organization shares data with another organization: You will need to be able to notify any organization you share data with if you find out that the personal data that your share is inaccurate.

The GPDR Admin Manual details where you can find personal data in Nextcloud and how to secure and handle it.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

3/ Communicate privacy information with staff and users

In order to be compliant, you should **review your current data privacy notices** alerting your staff and/or users about the collection of their data. Identify what you don't inform people of when it comes to the use of their data.

Under the current law, privacy notices need to **notify users** of:
- **your identity**
- the **reasons** you gather their data
- which **use** you make of their data
- who it will be **disclosed** to
- if the data will be transferred **outside the EU**.

Under the GDPR, you additionally need to inform them of:
- the **legal basis for processing** the data you collect
- which r**etention periods** you apply
- whether the data of your users will be subjected to **automated decision making**
- the fact that your users have a **right of complaint** if they are unhappy with the way you implement any of these criteria
- in general, their **individual rights** under the GDPR.

The GDPR also requires you to **make sure these notices are concise and easy to understand** for everyone – try to use easy language and avoid using any technical or legal jargon.

See the GPDR Admin Manual for information on how to inform users about their rights and how you use data.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

4/ Make sure your procedures cover all personal privacy rights

You should know all the rights the GDPR grants to individuals and take measures in order to **respect those rights**. These are the rights that are granted by the GDPR:
- **the right to be informed** of which data you retain and how it will be processed
- **the right to access** the data retained by your organization
- **the right to rectification** of the data you store
- **the right to erasure** of one's personal data
- **the right to restrict processing**; of one's personal data
- **the right to object** to data retention or processing
- **the right not to be subject to automated decision-making**, including profiling
- **the right to data portability**.

Note that the right to **data portability is new**, and only applies in three specific cases:
- personal data a person has provided to a controller
- in cases where the processing is based for the performance of a contract or on the person's consent
- if processing is carried out by automated means.

It is essential for your organization to consider if procedures you apply respect these rights, and whether you need to **make changes in order to be GDPR compliant**.

Making sure all these rights are respected includes figuring out in advance **how personal data is deleted**, and being able to inform users or staff of the way this is done. It also includes figuring out in advance how you will **provide personal data electronically** in cases where your users ask for it; you need to be able to provide this data **in a commonly used format**.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

5/ Be able to handle access requests

The GDPR brings changes in how your organization has to deal with **subject access requests**. In order to be compliant you should **review and update your current procedures** to handle those access requests.

You should be aware of the new timescales: While you currently have 40 days to comply to access requests, under the GDPR this time will be reduced to **a month**.

The GDPR requires you to give individuals making access requests **additional information** such as the data retention periods applied by your organization and their right to rectify the data you retain if it is inaccurate.

Generally you are **not allowed to charge** for complying with such a request. However you can refuse or charge for a request if you can demonstrate that the cost for your organization will be excessive, or if the request is manifestly unfounded. If you refuse a request, you will have to clearly communicate your refusal, and inform the person of the reasons for it. Additionally, you will have to inform the person of their right to complain to the supervisory authority in charge, and to a judicial remedy. Refusals must be communicated within one month at the latest.

If your organization handles a large amount of access requests, you should be prepared to deal with the impact of these changes. Providing additional information and dealing with requests in a shorter timeframe will **cost your organization a lot of time**. If needed, consider developing automated systems for people to access their information online.

Data in Nextcloud can be found in various areas. See the GPDR Admin Manual for an overview of those locations and how to extract the data.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

6/ Know the legal basis for processing personal data

Have you thought about your organization's **lawful basis to process personal data**? If not, you should do so in order to be GDPR compliant.

It is essential that you look at the **various types of data** carried out by your organization. The legal basis for processing data is generally the same before and under the GDPR. However, its practical implications are changed by the GDPR as individual rights are modified depending on your legal basis for processing their data.

This too needs to be **addressed in your privacy notice**: You will need to explain your legal basis for processing user data. Additionally, you will have to **mention it when answering a subject access request**.

When there is no specific legal basis for you to process personal data, you will have to **rely on consent** as a legal basis. This means that individuals will have a stronger right to have their data deleted or modified, as **consent can be withdrawn**.

If possible, **reduce the amount of types of data you retain**, as every data type you collect will have to be justifiable. You should consider **anonymizing** and/or **pseudonymizing** any type of data you don't need to store in a raw format.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

7/ Make sure you obtain consent to process data

If the legal basis you rely on to process personal data is consent, you should make sure **the way you obtain consent** follows the standards of the GDPR.

Review how you seek, manage and record consent and make the necessary changes. According the the GDPR, consent must be f**reely given, specific, informed and unambiguous**.

This means that:
- Users **cannot be forced** into consent.
- Users must be **aware** of what they consent to in terms of data processing.
- **Silence and inactivity** don’t mean explicit consent.
- **Pre-ticked boxes are not enough** to express explicit consent.
- Consent has to be **verifiable**.
- People must be **informed of their right to withdraw the consent** they have previously expressed and be able to do so in a simple way.
- Obtaining consent should happen in a way that is **separated from other terms and conditions**.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

8/ Be especially careful when processing children’s data

Is your organization likely to process **data from children**? If this is the case, you should put systems in place to verify if your user’s age, and obtain parental consent to process the data of underage subjects.

The GDPR will introduce **specific protections for the children’s personal data**, particularly in the context of social networking and commercial internet services. Under the GDPR, children will be able to give their own consent to data processing at 16, but some states can change this age limit, so make sure you know which age limits apply to the country you operate in. Under this age, you will need to obtain **consent from a person holding parental responsibility** – a parent or a legal guardian.

Here again, **consent needs to be verifiable**. This means that all rules set in step 7 of this guide must be followed, along with a notice in a language the underage subject can understand.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

9/ Know how to deal with data breaches

When it comes to dealing with the risk of a **data breach involving personal data**, the right procedures need to be put in place by your organization as soon as May 25th, 2018. Figuring out how to deal with a data breach when it happens is **too late** under the GDPR.

The procedures to deal with a data breach involve **detecting a breach, reporting it and investigating it**.

Under the GDPR, **breach notifications will be mandatory** for all organizations. Not all types of data breaches need to be reported: It is the case when breaches that are likely to result in a harm to the right and freedoms of individuals and could cause significant social or economic disadvantage to any individual whose data you retain. For example, this concerns be breaches that could result in financial loss, damage to reputation, etc.

Such data breaches must be **reported to the information officer** in charge in the country you operate in – make sure you are aware of the steps to follow in order to do this locally, and the timeline you will have to operate on. Such data breaches also need to be **reported to any individual concerned** by the breach.

Failure to report data breaches can result in fines: It is essential to set up a procedure in order to react in a timely manner.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

10/ Learn about Data Protection Impact Assessments (DPIA) and Data Protection by Design

The GDPR introduces mandatory privacy by design, called **“data protection and design and by default”** in the law. In short: Make the setting of your services as privacy-friendly as possible.

The GDPR also makes **Data Protection Impact Assessments** – short DPIA – mandatory in specific circumstances:
- with the deployment of a new technology
- when special categories of data are processed on a large scale
- with profiling operations that are likely to affect the privacy of individuals.

When making a DPIA, your organization systematically assesses the **potential impact your data processing could have on the privacy on people whose data you retain**, for each separate project of your organization. By making a DPIA your organization will be able to know if the processing operations carried out by your organization are GDPR compliant.

If you have to conduct a DPIA for a specific project, the questions you should ask are:
- Who will be in charge of the project?
- Who else will be involved?
- Will the process be run centrally or locally?

If you find out after a DPIA that your organization may not be able to be able to comply with the GDPR with full certainty, it is mandatory to notify and consult the authorities in charge in the state you operate in on the specific process that is at risk.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

11/ Consider designating a Data Protection Officer

Not all organizations have to designate a data protection officer under the GDPR. It is, however, essential to **find out if having a data protection officer is mandatory for your organization**.

If your organization is a public authority, if your organization carries out regular and systematic monitoring of individuals on a large scale or if your organizations processes sensitive data (health records, information about criminal conviction, etc.) on a large scale, you will have to designate a data protection officer. The data protection officer's role is to **take responsibility for your data protection compliance**, based on their knowledge of the topic, and has the support and authority to carry out this role ; this role with sit within your organization's structure and governance arrangements.

12/ Know about the rules regarding cross-border processing

This last step is only relevant **if your organization operates in more than one EU state**. In this case, you should determine which is your Lead Supervisory Authority for data protection and document it: The LSA is the supervisory in the state where your central administration or main establishment in the EU is.

Under the GDPR, your organization will **deal with a single LSA for most of your processing activities**. In order to find out what your main establishment is, start by mapping out where the **decisions about data processing** are made in your organization. This should indicate where which state's LSA you will depend on.

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

T: +49.711.25 24 28 -0
F: +49.711.25 24 28 -20

Web: https://nextcloud.com
E-Mail: sales@nextcloud.com

Conclusion

The GDPR is a complicated piece of legislation meant to combine a patchwork of local rules into one, definitive consumer protection law. It does much to protect privacy of users, forcing organizations to have a hard look at their policies and the way they deal with data. Especially when data leaves the organization, compliance becomes a headache, which is why self hosting with Nextcloud is among the easiest ways of ensuring compliance with the GDPR and similar laws across the globe.

There is much more to read about the GDPR. Two great documents can be found here:
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
http://gdprandyou.ie/gdpr-12-steps/
and you can find the text of the GDPR easy to search through here:
https://gdpr-info.eu/