# The cloud and cloud computing: what is it and how do you use it securely?

Cloud services offer many options for storing your digital archive without needing a hard drive or server. There are pros and cons to this.  
In this article, you’ll learn:

* What is cloud computing and how can you use it for your document management?
* What are the advantages and disadvantages of using the cloud?
* How can you minimise the risks of cloud computing?



All kinds of artists and arts organisations are using the cloud these days. Platforms such as Google Drive, OneDrive and Dropbox allow you to store your files centrally, so you don’t need your own server. This saves space on your own computers or external hard drives, often at no extra cost, and also makes it easy to share digital files with third parties.

But what is the cloud and cloud computing, exactly? What are the pros and cons? And how can you store your files as securely as possible there?

**Table of contents**

## **What is cloud computing?**

*Cloud computing* enables computing services to be made available on demand via a network, usually the internet. Even though this gives end users a virtual, scalable infrastructure, they don’t own it, and so aren’t responsible for maintaining and updating the data, software and hardware themselves. They don’t know how many or which computers their data is stored on, or where the software is running, or even where the computers are located.

The *cloud* is the network of connected computers required to provide these services. Companies that supply cloud computing services are called cloud providers, and they usually charge fees based on usage.

## **What is cloud computing useful for?**

If you use online services to send emails (e.g. Gmail), edit documents (e.g. Google Docs or Microsoft Office 365), watch films or TV programmes (e.g. Netflix), listen to music (e.g. Spotify or iTunes), play games (e.g. Xbox Live or PlayStation Now) or save photos and other files (e.g. iCloud, Dropbox or Google Drive), you are already using cloud computing behind the scenes. Private individuals as well as companies, government institutions and non-profit organisations all use cloud services, for example to:

* create new applications and services;
* save data, make back-ups and restore files;
* analyse data and make forecasts;
* host websites and blogs;
* stream audio and video;
* provide software on demand.

## **How does cloud computing work?**

On one hand there’s the *front end*, which is the computer user or customer side, and on the other there’s the *back end*, which is the computers, servers and data storage systems that together form the cloud. These are all connected to each other through a network, usually the internet. The way in which cloud computing services are supplied can differ from one *provider* to the next.

Services such as web-based email programs (e.g. Gmail) use existing web browsers for the front end, and many professional cloud computing services have user-friendly dashboards (e.g. Google Admin console for Google cloud services), accessed via browsers, to order services and manage *accounts*. A central server manages the system and controls traffic and client requirements to ensure everything runs smoothly.

There are different types of cloud computing services, but regular users will mainly encounter what is known as *Software as a Service* (SaaS), which enables you to use a cloud provider’s software applications, usually on a subscription basis. The software is provided, managed, maintained and updated by the provider, and examples include Office365, Gmail, Hotmail, Google Drive and Dropbox.

## **How is the cloud implemented?**

There are three different ways to implement cloud computing:

1. Public cloud. A cloud provider owns and is responsible for maintaining all the hardware, software and other support infrastructure. Access to services and account management takes place via a web browser. When you use Google Drive, Dropbox, OneDrive or Amazon Web Services for storage, you’re using a public cloud.
2. Private cloud. This cloud infrastructure is installed and used exclusively for your own organisation. Its management is taken care of internally or outsourced to a third party.
3. Hybrid cloud. This combines public and private clouds, linked together so information and applications can be shared. In practice, private clouds cannot normally exist separately from the rest of an organisation’s IT infrastructure and the public cloud; they use a combination of data centres, private clouds and public clouds, and are therefore called hybrid clouds. Data and applications can be moved between these clouds, which offers more flexibility and possible implementations.

## **Why should you use the cloud?**

### **Costs**

With cloud computing, you no longer need to invest in your own hardware and software, or set up and manage your own data centres. It also helps to keep licensing costs down, which can otherwise increase rapidly for multiple users. The cloud is therefore often cheaper with scalable options (e.g. pay per use). Google Drive, OneDrive and Dropbox all allow you to benefit from free storage, so you don’t need to invest in buying your own external hard drive.

### **Easy access**

It is easy to share and use files and software. You have access to your applications and information wherever there’s an internet connection, and can easily share your files in public clouds simply by sending links to third parties. You can also save certain cloud applications, such as Dropbox and Google Drive, locally on your own computers to have access to information without an internet connection. Access is no longer limited to a specific geographical location.

### **Scalability**

Cloud computing services offer flexible scalability. Computing power, storage capacity and bandwidth can all be tailored to current demand and geographical location. Cloud storage enables almost unlimited storage capacity.

### **Speed**

You can use cloud applications as soon as you have registered or made a payment. You no longer need to install your own software, which can also result in significant time savings.

### **Reliability**

Cloud computing makes backing up data, emergency restoration following a disaster, and safeguarding business continuity easier and cheaper. Data can be stored in deduplicated form at multiple locations in the cloud provider’s network, and providers should be competent enough to execute any emergency restoration themselves. They also regularly update their products to the most recent, fast and efficient hardware, so you no longer need to be responsible for this.

## **What are the risks?**

### **Lack of support**

Customer support offered by cloud services isn’t always optimal, which can result in longer than acceptable waiting times.

### **Copyrights**

In some cases, you lose your rights to the content you store online.

### **Costs**

Cloud computing isn’t always as cheap as it might seem, and cheaper cloud solutions might not have all the features you need. The free versions of Google Drive and Dropbox, for example, only have limited functionality and storage capacity. You have to pay a monthly subscription if you want more storage, or perhaps use your own domain name. Data also isn’t protected as securely in free versions, and you have less time to restore deleted or modified files.

### **Security**

It’s possible that sensitive information is passed on to a third party (the cloud provider) when using cloud services, and this implies certain risks, which is why you should always choose the most reliable and trustworthy. Government institutions prefer to set up their own cloud servers because of restrictions placed on the data they manage.

Cloud storage also makes organisations more vulnerable to external attacks from hackers and other threats. And even the best cloud services can be susceptible to failure and other technical problems, despite their high maintenance standards. These problems could perhaps make applications such as Google Drive and Dropbox temporarily unavailable, so you wouldn’t be able to access your information temporarily.

In the summer of 2015, Google lost files as a result of four lightning strikes on their data centre in Belgium. 0.000001% of the files stored there couldn’t be restored again.[[1]](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/the-cloud-and-cloud-computing-what-is-it-and-how-do-you-use-it-securely#cite_note-1) This might not seem like much, but what if you lost your most important documents? It’s therefore best not to use the cloud as your only long-term data storage solution. And with cloud storage, you are also reliant on having a reliable internet connection.

There are a number of international standards for information security (ISO 27001), cloud security (ISO 27017) and personal data protection in the cloud (ISO 27018):

* ISO 27001 is an international standard for information security, including risk analysis and restore operations. The standard is based on best practices for the protection of information systems set out in the international standard ISO 27002.
* ISO 27017 was developed because ISO 27001 wasn’t satisfactory for cloud applications. It’s an international standard for the protection of cloud applications.
* ISO 27018 is an international standard for personal data protection in the cloud.

Service providers that satisfy these three standards guarantee a secure system with a back-up strategy and restore procedures, where your personal data is securely protected. Commonly used cloud systems, such as Google Drive and Dropbox, support these standards in paid versions but not in the free versions. If you use the free version, this therefore means that Google or Dropbox cannot guarantee that your files won’t become lost.

Human error is another significant threat to protecting your digital files in the cloud. Google Drive and Dropbox are platforms that allow collaboration on documents. Someone you share a folder with can therefore edit, delete or add files in this folder, which could be a risk for your digital collection. If someone accidentally deletes a file, for example, and you don’t notice in time, you have lost this file irrevocably unless you’ve made a back-up.

For small organisations, switching to the cloud can result in improved security because large cloud providers achieve security levels that they could never reach themselves.

## **How can you protect yourself against the risks?**

### **Appoint a manager**

Make someone responsible for managing files in the cloud, to ensure nothing is deleted or edited unintentionally. They will have the permissions required to add and delete files, and decide who files are shared with. Appointing a manager means you can be certain that at least one person will check the folder for irregularities, and that files cannot be edited, deleted or added by just anyone, which reduces the risk of human error.

### **Change your password regularly**[**[2]**](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/the-cloud-and-cloud-computing-what-is-it-and-how-do-you-use-it-securely#cite_note-2)

Popular cloud services have become victim to hacking on a few occasions before. In 2012, for example, a security breach at Dropbox exposed 69 million users’ email addresses and passwords.[[3]](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/the-cloud-and-cloud-computing-what-is-it-and-how-do-you-use-it-securely#cite_note-3) It is therefore important to change your password regularly, and use a unique password for each service. It’s much more difficult to crack a password that uses a minimum of 8 characters and a combination of numbers, letters and punctuation marks. Read more about this in the [Keeping passwords secure](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/safe-use-of-passwords) section.

### **Analyse your files**

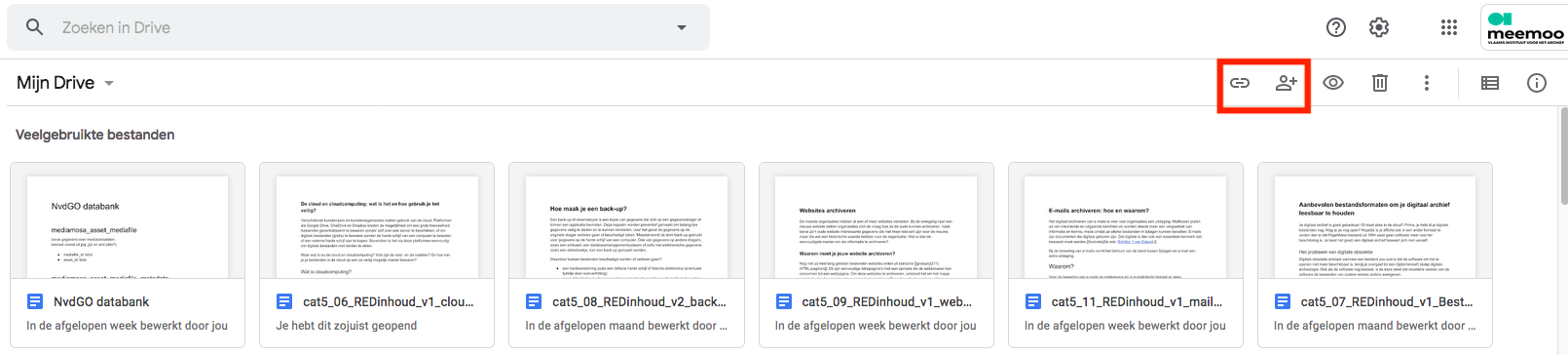
Considering that Google Drive, OneDrive and Dropbox are collaborative platforms where third parties can view, edit and delete documents, it’s best to make a distinction between files you collaborate on (such as reports, work and accounting documents), and files that can only be looked up (such as digitised photos, magazines and newspapers). Synchronisation is after all an important concept for cloud systems such as Dropbox, Google Drive and OneDrive.

Synchronisation is when you have a folder on your computer that contains files, and the online service ensures that the contents of this local folder are always synchronised with the online location (and vice versa). This has the advantage that you can work on your files offline and, when you have an internet connection again, automatically update your files in your online location, so you’re never working with different versions. Synchronisation also has the disadvantage, however, that you also delete a file from your online storage if you accidentally delete it from your local folder.

It can therefore be better to use cloud back-up and storage services, such as Amazon Web Services or RackSpace, for files that do not need to be edited and are saved in the cloud purely as for back-up purposes. There is no synchronisation in this case. You hire storage capacity from an online service and save your files there, similar to when you might rent storage space in a warehouse for household items.

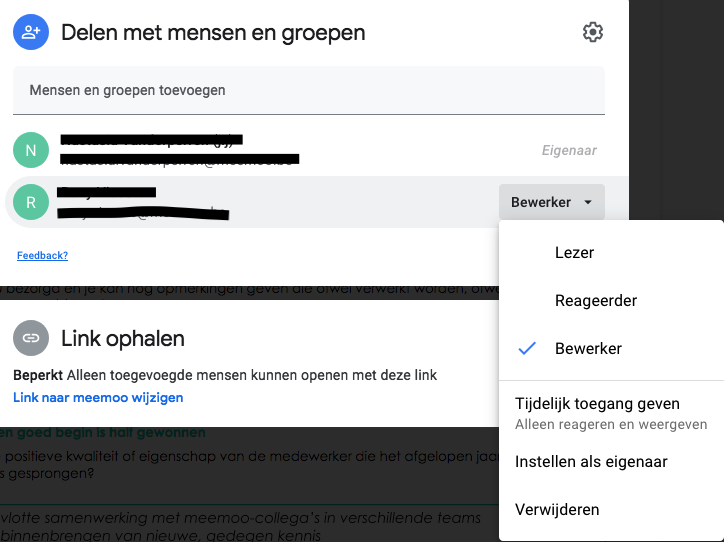
If you do choose to save files in Dropbox, Google Drive or OneDrive, however, it’s best to only give third parties reading rights for the reference files (such as digitised photos or magazines) that you share with them, to prevent them from being able to edit or delete files.

* In Google Drive, you can use the buttons inside the red frame to share files and set access rights. The left button generates a link for sharing a file, and you can use the right button to give access rights to specific people.

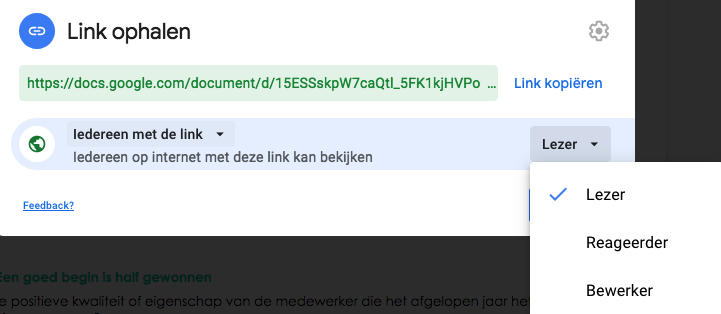


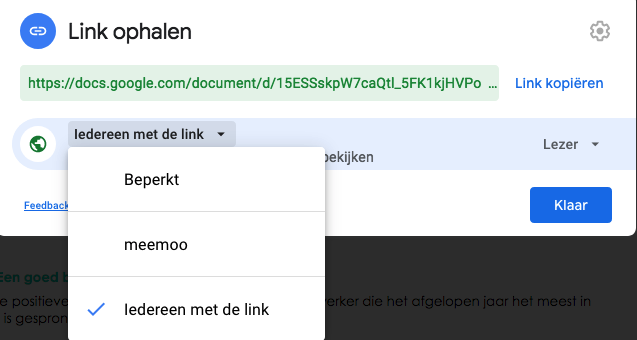
* When you want to share a file with specific people, you see the following window. Enter the email address for the person you want to share the file with, and select what this person is allowed to do with this file: read or edit.



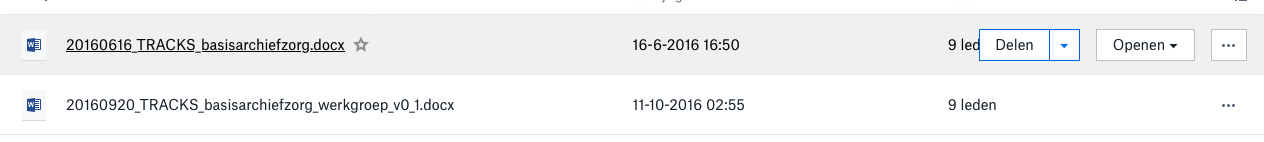


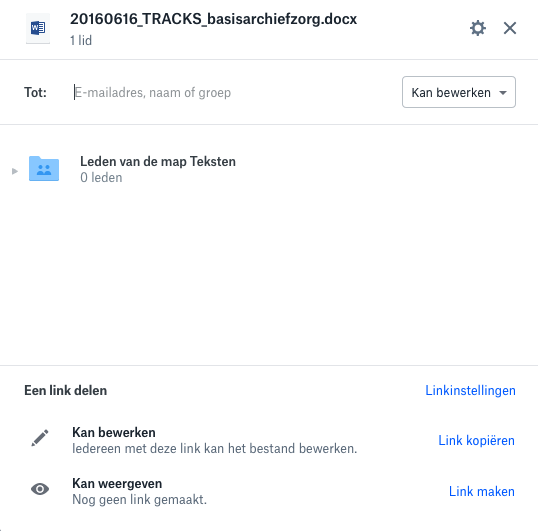
* You can also choose what access rights the users have when you share an entire folder with third parties. We will share an entire folder here.



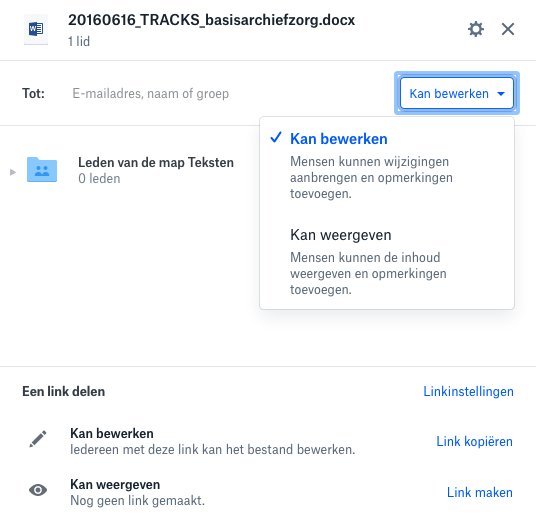


* You can also share files and folders and assign access rights with Dropbox.





* Just like in Google Drive, you can create a link to share files or folders or provide access to specific people. The difference with Google Drive is that you cannot share individual files with editing rights in Dropbox. Only folders can be shared with editing rights.



In order to make it easier for yourself, you can place the files to be edited in different folders from the files not to be edited. You keep reference files in a reference folder which you share with reading rights, and keep files that can be edited in a different folder, with writing rights shared only with authorised persons.

### **Make back-ups**

Just like all the other files in your digital archive and collections, files in the cloud also need to be [backed up](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/how-do-you-make-a-back-up). This prevents you from losing files if they are accidentally deleted, edited or damaged. A good back-up strategy ensures that files are saved on different technology in at least two different geographical locations. You should not therefore store all your files with a single cloud service. Make sure you also have local storage on your own computer or server.

One way of backing up your files in the cloud is to make back-ups of your local folder. If you make a back-up via Windows Back-Up, Time Machine or another application, you always have an external copy of these files. There are also cloud services that make cloud-to-cloud back-ups of your Google Drive, such as [Backupify](https://www.backupify.com/), [Spinbackup](https://spinbackup.com/) and [Spanning](https://spanning.com/).

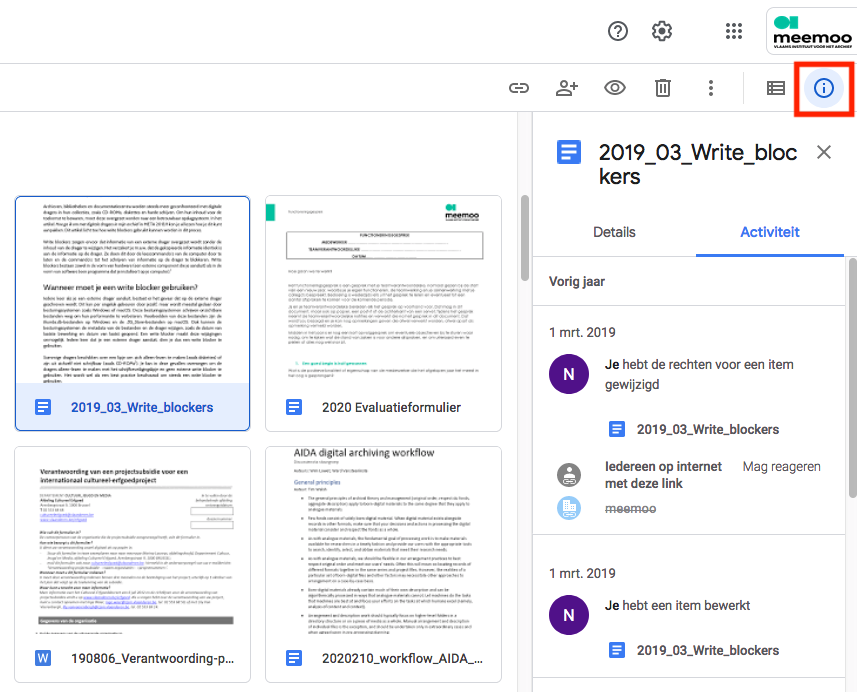
### **Make checksums**

You can use [checksum tools](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/checksums-as-a-way-to-preserve-file-integrity) to automatically check if files have been modified, deleted or added. If you configure this tool to check your files automatically, you receive an email whenever a file is modified, deleted or added. This enables you to automatically check if your folder is still complete and unchanged without needing to check each document manually.

### **Check versions**

If you notice that a file has been modified, you can check what changes have been made via your cloud platform. Dropbox and OneDrive have dashboards that show any modifications to your shared files, and with Google Drive you have a sidebar to check a file’s status. Google Drive, Dropbox and OneDrive all offer the possibility of reversing any changes and returning to previous versions. You have 30 days to do this.

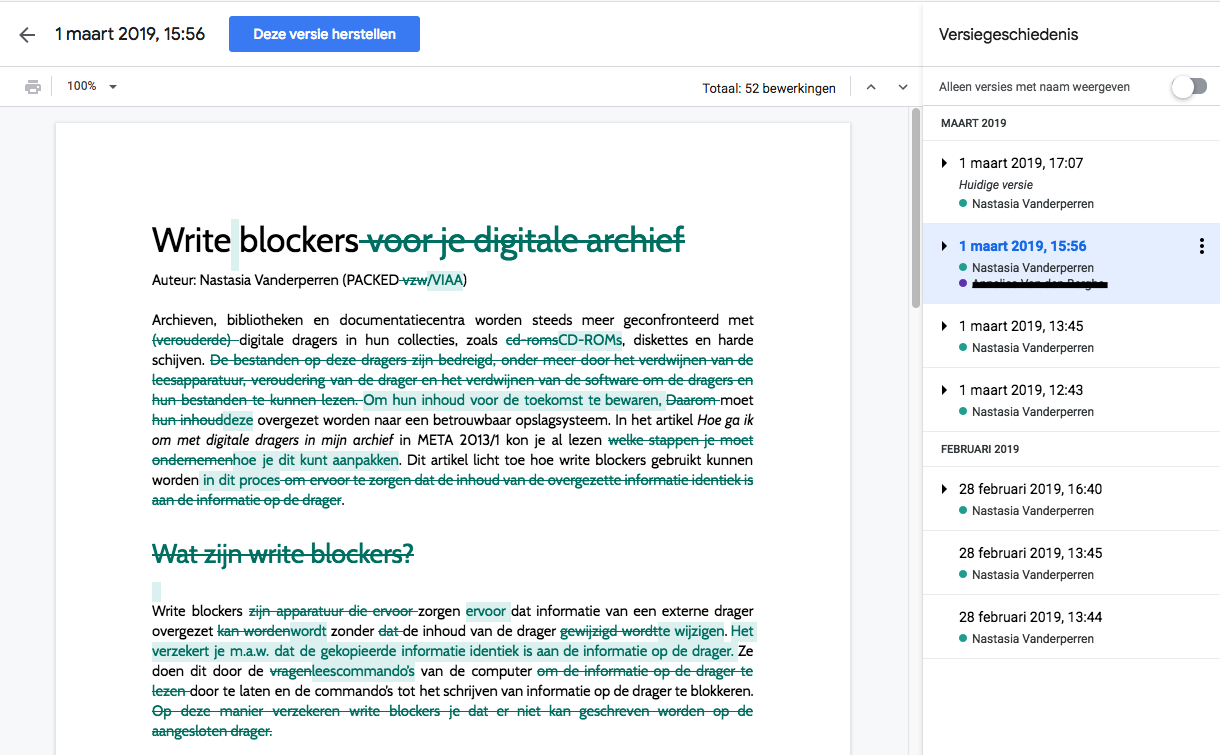
* In Google Drive, you can see activities and details for a document by clicking on the info button.



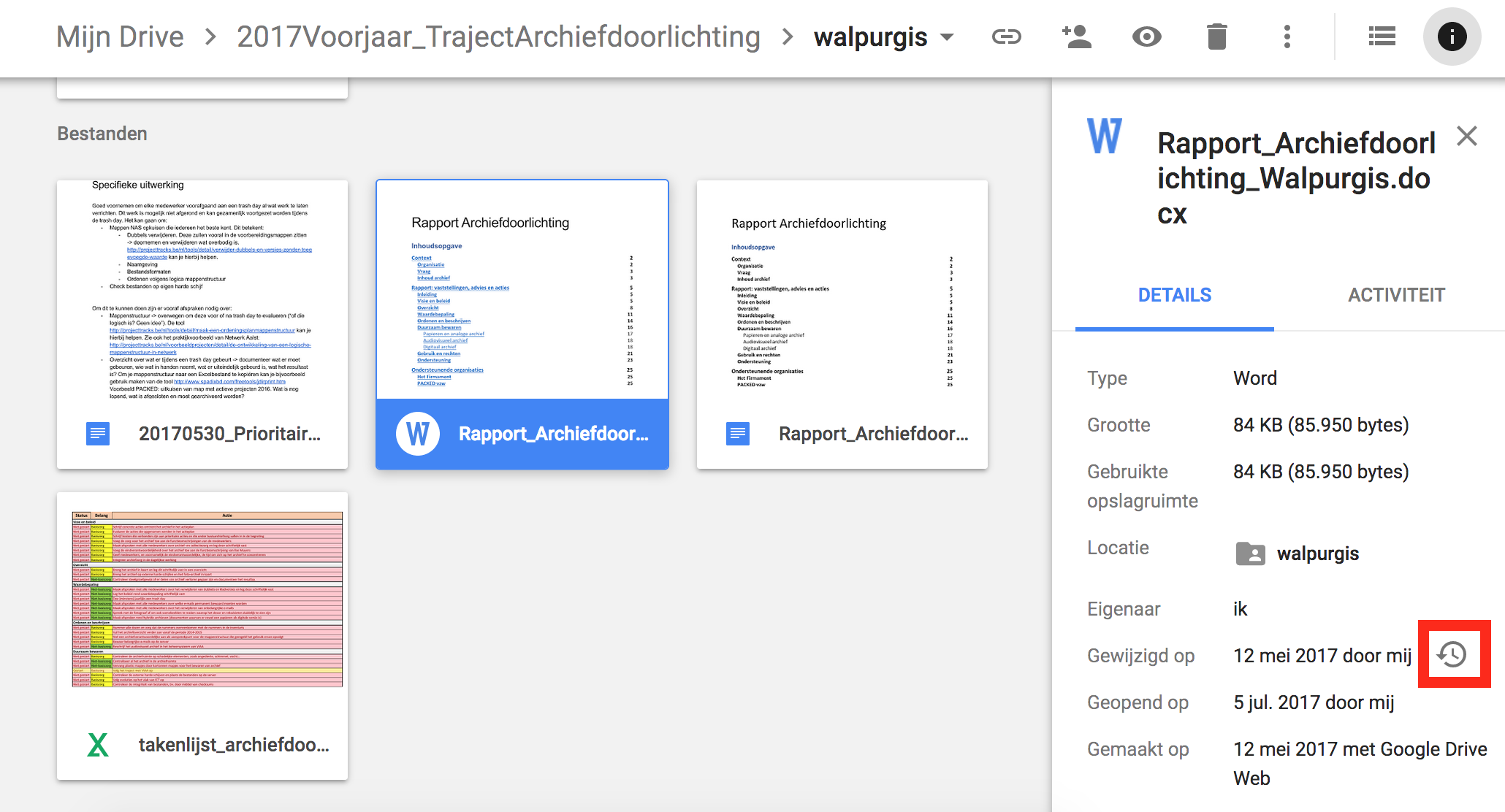
* You can see all changes in a Google document by clicking on ‘All changes saved in Drive’.



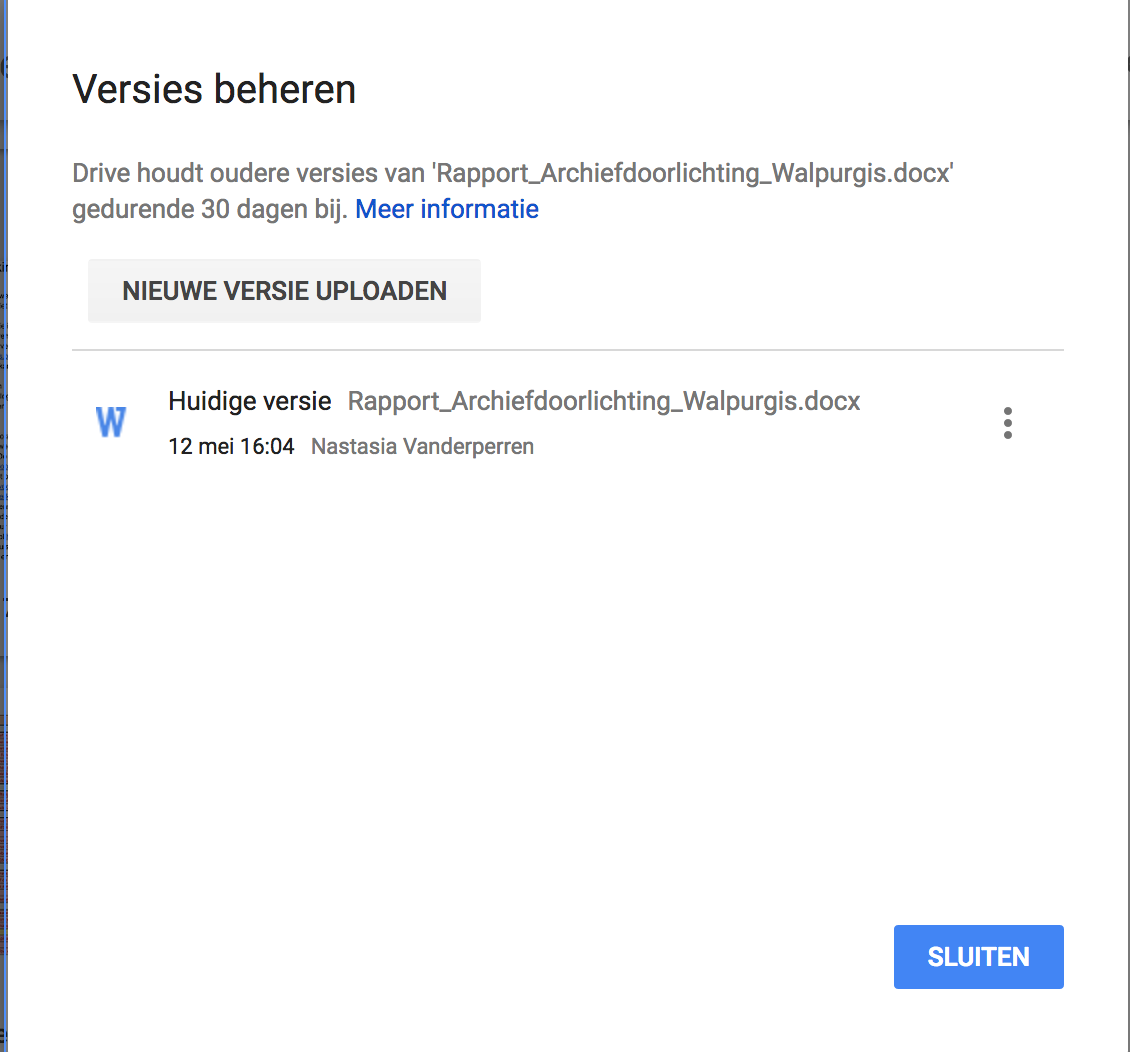
* The coloured text is the modified text. If you wish, you can return to a previous version.



* Multiple versions of documents that have been uploaded, such as photos, text files and spreadsheets, can also be saved.



* You can see the different versions by clicking on the symbol next to ‘Modified on’. You can upload new versions or restore old versions. Please note: Google Drive only saves the various versions of uploaded documents for 30 days.



## **Conclusion**

Cloud storage makes it possible to save files and share them with third parties securely. There are still risks related to the sustainability of your digital collection, however. It is therefore better to use cloud storage as part of your storage strategy, but do not rely on it for your whole strategy. The type of cloud storage you choose also depends on your particular wishes. It’s always important to weigh up the pros and cons. You can use this matrix to compare the three services.[[4]](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/the-cloud-and-cloud-computing-what-is-it-and-how-do-you-use-it-securely#cite_note-4)

|  | **Google Drive (free)** | **Dropbox (free)** | **OneDrive (free)** |
| --- | --- | --- | --- |
| **How to use?** | Via Google Account. No software installation required. | after software registration and installation. | Via Microsoft Account. No software installation required. |
| **Storage** | 15 GB[[5]](https://www.projecttracks.be/en/toolbox-overview/digitaal-bewaren/the-cloud-and-cloud-computing-what-is-it-and-how-do-you-use-it-securely#cite_note-5) | 2 GB | 5 GB |
| **Sharing** | * via a link that you can share with others. Other people can also use this link to share the file or folder with third parties. * via an email invitation to specific people. * reading, commenting and writing rights can be allocated at folder and file level via a link and via email. * via a link that you can share with others. Other people can also use this link to share the file or folder with third parties. * Writing and reading rights can only be allocated at folder level | * via a link that you can share with others. Other people can also use this link to share the file or folder with third parties. * via an email invitation to specific people. * access rights (reading and writing rights) can only be restricted via email invitation. |  |
| **How much time do you have to restore deleted files?** | Deleted files are saved in the recycle bin. As long as the files have not been deleted from there, they can always be retrieved. | 30 days. | 30 days. When the size of your recycle bin reaches 10% of your OneDrive folder storage, the biggest files are deleted within three days and are not saved for 30 days. |
| **Version management** | Version management is supported. A maximum of 100 versions are saved for files that have not been created using Google applications. You can restore previous versions for up to 30 days after editing.  You can see who has edited which file via the sidebar. | Version management is supported. You can restore previous versions for up to 30 days after editing.  You can see who has edited which files via a dashboard. | Version management is only supported for Microsoft files. You can restore these versions for up to 30 days after editing.  You can see who has edited which file via a dashboard. |
| **Local storage and synchronisation** | Yes | Yes | Yes |
| **Helpdesk** | * 24/7 live chat (with waiting times); * 24/7 telephone support (with waiting times); * via email; * via user forum; * via YouTube channel with help videos. | * via user forum; * online documentation with frequently asked questions; * contact page. | * online documentation with frequently asked questions; * via email; * virtual assistant. |

Authors: Nastasia Vanderperren (meemoo) and Rony Vissers (meemoo)