# Hoe bewaar ik mijn gegevens?

**Iedereen in Nederland krijgt belangrijke berichten via de post of digitaal. Hoe kun je deze belangrijke berichten het best bewaren? Wat zijn de voor- en nadelen van de verschillende bewaarmethodes? En wat zijn eventuele risico's?**

**In onderstaand schema staan de voor- en nadelen op een rij.**

| | Papier | Computer | E-mail-omgeving | Cloud | Externe gegevensdrager | Mijn-omgeving |
|---|---|---|---|---|---|---|
| Makkelijk deelbaar | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Altijd/overal in te zien | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Privacygevoelig | ✓ | ✓ | ✗/✓ | ✗/✓ | ✓ | ✗/✓ |
| Goed te beveiligen | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Duurzaam | ✗ | ✗ | ✓ | ✓ | ✗ | ✗/✓ |
| Brand of diefstal | ✗/✓ | ✗ | ✓ | ✓ | ✗/✓ | ✓ |
| Verlies of beschadiging | ✗ | ✗ | ✓ | | ✗ | ✓ |
| Virus of Ransomware | ✓ | ✗ | ✗/✓ | ✗ | ✓ | ✗/✓ |

✓ = Dit kan met deze bewaarmethode/de methode is hier niet gevoelig voor
✗ = Dit kan niet met deze bewaarmethode/de methode is hier gevoelig voor
✗/✓ = Dit kan, maar vereist extra actie (zie hierna)

## Op papier

Steeds meer berichten krijgen we digitaal, maar er valt ook nog post op de deurmat. Als je deze post netjes en gestructureerd opbergt, kun je dit eenvoudig delen met anderen, bijvoorbeeld je partner. Je hoeft niet bang te zijn voor hackers die via de computer bij jouw gegevens kunnen.

Nadelen van het bewaren van papier zijn er ook: bij brand, diefstal, verlies of beschadiging ben je het kwijt. Je kunt dit risico beperken door een brandvrije kluis te gebruiken.
Ook is het niet eenvoudig om gegevens te delen met iemand op een andere locatie. En het kan lastig zijn om iets terug te vinden (afhankelijk van de manier waarop je je papieren sorteert en opbergt).

## Op de computer

De bekendste manier van bestanden opslaan is het bewaren van persoonlijke documenten op de harde schijf van de computer. Dit kan ook op je tablet of mobiele telefoon, maar dat is minder overzichtelijk dan op een computer.

De bestanden worden *niet* online bewaard, waardoor anderen er niet zomaar van buitenaf bij kunnen. Toch is het aan te raden om goede anti-virus software en een firewall te installeren. Zo worden je gegevens beter beschermd. Op een computer zijn er meer mogelijkheden om deze beveiligingen te installeren dan op een tablet of mobiele telefoon.

Als je device (computer, tablet of telefoon) wordt geïnfecteerd met een virus, kun je (een groot deel van) je bestanden kwijtraken. Ook bij brand, verlies of beschadiging van het apparaat kunnen gegevens verloren gaan. Het is daarom aan te raden om regelmatig een back-up te maken op een externe gegevensdrager zoals een externe harde schijf of usb-stick, of bij een online opslagdienst (zie: 'In de cloud').

## In je e-mail-omgeving

Er zijn diverse aanbieders van e-mail-accounts. Sommigen zijn volledig online, andere accounts kun je installeren op je computer, laptop, tablet of telefoon. Omdat veel belangrijke berichten per e-mail worden verstuurd, is het een goede optie om berichten ook in de e-mailomgeving op te slaan.
Bij de meeste e-mail-accounts kun je mappen per onderwerp aanmaken, berichten archiveren en berichten doorzoeken met een zoekfunctie.
Berichten die je op papier ontvangt, kun je scannen en naar jezelf e-mailen. Je kunt deze post vervolgens opslaan in de cloud, op de computer, op een externe gegevensdrager of in je e-mailomgeving.

Bij een mailomgeving maak je gebruik van de diensten van een aanbieder en ga je akkoord met hun algemene voorwaarden. Dat kan betekenen dat je toegang geeft tot (een deel van) je gegevens. In het geval van een 'datalek' of een hacker kunnen gegevens worden gestolen. In de praktijk komt dit weinig voor.

## In de cloud

Je kunt ook documenten opslaan in de 'cloud'; op de internetserver van een clouddienst. Je hebt een computer, tablet of telefoon nodig om de bestanden te kunnen uploaden in de cloud.
De bestanden staan dan online (op internet) en zijn niet gebonden aan een apparaat. Het voordeel is dat je met een internetverbinding altijd en overal bij je gegevens kan en bestanden ook eenvoudig kunt delen.

In het geval van brand of beschadiging van een apparaat gaan je gegevens niet verloren.

Nadelen van cloud-diensten zijn mogelijke inbreuk op je privacy en risico op hacks. Je stemt in met de algemene voorwaarden van bijvoorbeeld Google of Microsoft en geeft zo toegang tot (een deel van) je gegevens. Je kunt ervoor kiezen om bestanden te versleutelen (encryptie) en met meerdere beveiligingsopties te werken (zoals sterke wachtwoorden of twee factor-authenticatie) om dit risico te verkleinen.

De voor- en nadelen van de meestgebruikte clouddienst-aanbieders op een rij:

### Dropbox

- 2GB opslagruimte gratis, tegen betaling of door acties uit te breiden
- Onbeperkt aantal apparaten te koppelen; beschikbaar voor desktop, mobiel en tablet.
- Mappen of losse bestanden zijn makkelijk deelbaar waardoor Dropbox ook geschikt is voor een gezamenlijke administratie.
- Twee factor-authenticatie mogelijk; goed te beveiligen
- Meer informatie op dropbox.com

### Google Drive

- 15GB gratis opslagruimte, tegen betaling uit te breiden.
- In combinatie met een Google-account makkelijk te combineren met andere Google-diensten.
- Onbeperkt aantal apparaten te koppelen; beschikbaar voor desktop, mobiel en tablet.
- Mappen of losse bestanden zijn makkelijk deelbaar waardoor Google Drive ook geschikt is voor een gezamenlijke administratie.
- Twee factor authenticatie mogelijk; goed te beveiligen
- Meer informatie: google.com

### Microsoft OneDrive

- 5GB gratis opslagruimte, tegen betaling uit te breiden. In combinatie met een Office pakket 1TB opslagruimte.
- Onbeperkt aantal apparaten te koppelen; beschikbaar voor desktop, mobiel en tablet.
- In combinatie met een Microsoft-account makkelijk te combineren met andere Microsoft-diensten.
- Twee factor authenticatie mogelijk; goed te beveiligen
- Meer informatie: onedrive.live.com

iCloud

- 5 GB gratis opslagruimte voor iedereen die tenminste 1 Apple-apparatuur heeft. Tegen betaling uit te breiden.
- Verder vergelijkbaar met de voorwaarden zoals de andere clouddiensten.
- Meer informatie: apple.com/icloud

## Externe gegevensdrager

Aan je computer of laptop kun je eenvoudig een externe gegevensdrager koppelen, zoals een externe harde schijf of usb-stick. Je kunt zelf kiezen hoeveel opslagruimte je nodig hebt en waar je de gegevensdrager bewaart. Je kunt de gegevens eenvoudig meenemen en - indien gewenst - bepaalde mappen versleutelen. Het delen van de gegevens gaat minder makkelijk dan via een cloud-dienst, maar het is wel mogelijk.

Je kunt de externe harde schijf ook koppelen aan het wifi-netwerk thuis en zo een 'netwerkschijf' maken. Dit is echter niet eenvoudig.

Externe gegevensdragers kunnen vatbaar zijn voor brand, diefstal, verlies of beschadiging. Je kunt het risico op brandschade of diefstal beperken door een brandvrije kluis te gebruiken.

## Mijn-omgeving

Veel energiemaatschappijen, zorgverzekeraars en overheidsinstanties (maar ook bedrijven zoals telecom-aanbieders) bieden een mijn-omgeving aan. Een mijn-omgeving is een gepersonaliseerd deel van een website, waar je toegang toe hebt via een persoonlijk account en wachtwoord. In het geval van overheidsdiensten kan dit ook je Digi-D zijn.

Vaak worden deze mijn-omgevingen gebruikt om berichten met je te delen. Denk aan een polisoverzicht of een jaarafrekening van het waterverbruik. Je kunt de mijn-omgevingen ook gebruiken om informatie in op te slaan en/of te archiveren. Zo bewaar je de informatie per aanbieder bij elkaar en hoef je geen papieren te bewaren.

***Let op:*** deze mijn-omgevingen kun je meestal alleen gebruiken als je klant bent. Als je bijvoorbeeld overstapt naar een andere zorgverzekeraar, dan is de mijn-omgeving van je vorige zorgverzekeraar vaak nog maar een beperkte periode voor jou toegankelijk.