

# Informatie voor (nieuwe) medewerkers

## *Privacy en informatiebeveiliging*

### Het begint bij jou

Binnen de VU vinden we het belangrijk de persoonsgegevens van onze studenten, medewerkers en anderen zoals onderzoekdeelnemers goed te beschermen. De VU is wettelijk verplicht om ervoor te zorgen dat persoonsgegevens veilig en zorgvuldig worden verwerkt. Voor iedereen is hier een rol weggelegd.

### 1. Wat moet ik doen?

Privacy kan niet bestaan zonder informatiebeveiliging. De Dienst Informatietechnologie (IT) bewaakt ons netwerk continu, maar informatiebeveiliging heeft meer nodig. Wees je ervan bewust dat informatiebeveiliging bij jou begint. Wij vragen je daarom om in ieder geval de volgende regels te volgen.

#### Data delen en e-mail

1. Verstuur gevoelige informatie altijd met een beveiligd systeem (ook intern). Hiervoor is Zivver of SURF Filesender beschikbaar. Zie voor een handleiding: [Zivver](#) en [SURFfilesender](#).<sup>1</sup>
2. Verstuur externe groepsmails met de mailadressen in de BCC.
3. Controleer of je de juiste en niet te veel contactpersonen hebt geselecteerd.
4. Laat uitgeprinte documenten nooit op de printer of een onbeheerde plek liggen.
5. Gebruik passende opslaglocaties voor (gevoelige) gegevens. Neem bij twijfel contact op met de [IT-servicedesk](#).



#### Apparaten

6. Vergrendel je computer bij korte afwezigheid en log uit of sluit af bij langere afwezigheid. (Windows: Windowstoets + L of Mac: Command + Control + Q)
7. Let extra goed op je apparaten in openbare ruimtes zoals in de trein of in een café.
8. Laat je apparaat niet onbeheerd achter. Gebruik indien mogelijk een laptopkabelslot.
9. Gebruik geen (onversleutelde) mobiele opslagmedia zoals usb-sticks, mobiele harde schijven, e.d.
10. Update je computer, telefoon of tablet zo snel mogelijk. Wacht daar niet mee.<sup>2</sup>
11. Zorg ervoor dat de harde schijf van de computer waarmee je werkt is versleuteld (bijvoorbeeld [Bitlocker](#) of [Filevault](#)). Neem bij vragen contact op met de [IT-servicedesk](#).

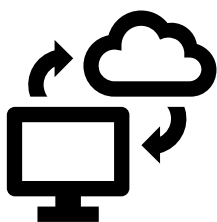
#### Wachtwoorden

12. Deel nooit je wachtwoord. Medewerkers van de Dienst IT zullen ook nooit naar wachtwoorden vragen.
13. Gebruik een sterk wachtwoord of een wachtzin. Voor tips, klik [hier](#).
14. Gebruik je VU-wachtwoord niet voor andere accounts.

---

<sup>1</sup> Indien de link niet correct werkt, copy/paste de URL dan in je browser.

<sup>2</sup> Bij beheerde werkplekken wordt dit door de Dienst IT verzorgd.



### Internet, WiFi en VPN

15. Klik niet zomaar op links. Bij twijfel of een webpagina, mail of link phishing is, vraag het de [IT-servicedesk](#).

16. Maak geen gebruik van openbare WiFi-netwerken. Als een openbaar wifinetwerk onvermijdelijk is, gebruik dan een VPN (zoals [EduVPN](#)) en verwijder na gebruik het openbare netwerk van het apparaat.

### Bewaartermijnen

17. Gegevens mogen niet langer worden bewaard dan noodzakelijk. De afdeling Document Management en Archief (DMA), onderdeel van de Dienst Bestuurszaken (BZ), heeft daarom [bewaartermijnenlijsten](#) opgesteld waarin je kan terugvinden wat de bewaar- en vernietigingstermijnen zijn.

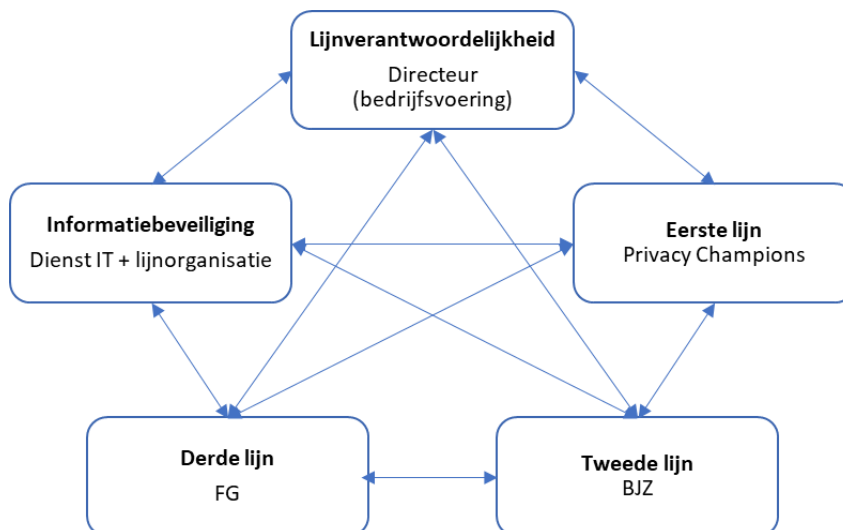
### Datalekken

18. Het is belangrijk dat eventuele datalekken snel na ontdekking worden gemeld, zodat de juiste maatregelen kunnen worden genomen. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een mail met persoonsgegevens die per abuis naar een verkeerde ontvanger wordt gestuurd. Een datalek kan ook zijn een inbraak in een databestand door een hacker en/of door kwaadaardige software, die een computer of bestanden gijzelt. Ernstige datalekken moeten binnen 72 uur na ontdekking door de VU aan de Autoriteit Persoonsgegevens worden gemeld.

Neem bij een datalek of vermoeden daarvan **direct** contact op met de IT Servicedesk via 020-59 80000 of [servicedesk.it@vu.nl](mailto:servicedesk.it@vu.nl). Meer informatie vind je op [VUweb](#).

## 2. Hoe is het onderwerp privacy geregeld binnen de VU?

De VU is een grote organisatie is die veel (gevoelige) persoonsgegevens verwerkt. Om die reden heeft de VU ervoor gekozen om privacy gedeeltelijk centraal en gedeeltelijk decentraal te organiseren.



### Lijnverantwoordelijkheid

Het voldoen aan de privacywet- en regelgeving is binnen de VU een lijnverantwoordelijkheid. Dat houdt in dat de Directeur van een Dienst of de Directeur Bedrijfsvoering van een Faculteit eindverantwoordelijk is dat haar of zijn eenheid voldoet aan de wettelijke vereisten.

**Eerste lijn: Privacy Champions**

Elke Faculteit of Dienst heeft één of meerdere [Privacy Champions](#). De Privacy Champions zijn medewerkers die door de Faculteiten en Diensten van de VU zijn aangesteld om eerste aanspreekpunt te zijn bij het beantwoorden van vragen op het gebied van privacy en gegevensbescherming. De Privacy Champions weten wat er op hun afdeling speelt, waar in de praktijk behoefte aan is en hoe zaken binnen de eenheid zijn geregeld. De Privacy Champions kunnen daar waar nodig snel schakelen met de privacyjuristen voor advies.

**Tweede lijn: Bestuurlijke en juridische zaken**

De afdeling [Bestuurlijke en Juridische Zaken](#) (BJZ) is de afdeling binnen de Dienst [Bestuurszaken](#) (BZ) die is belast met de organisatie van, en de advisering over, bestuurlijke en juridische aangelegenheden. De privacyjuristen houden zich bezig met het gevraagd en ongevraagd adviseren over het privacyrecht zodat we zo goed mogelijk aan de AVG en andere (privacy-)wetgeving voldoen.

Je kan het privacyteam van BJZ bereiken via [privacy@vu.nl](mailto:privacy@vu.nl).

**Derde lijn: Functionaris Gegevensbescherming**

De [Functionaris voor Gegevensbescherming](#) is de interne toezichthouder op het gebied van privacy en de bescherming van persoonsgegevens. De FG rapporteert rechtstreeks aan het College van Bestuur (CvB). De FG is verder het eerste aanspreekpunt voor betrokkenen (de personen van wie de VU persoonsgegevens verwerkt) en coördineert het proces bij [datalekken](#).

**Reglementen en beleid:**

De VU heeft ook reglementen en beleid op het gebied van privacy en informatiebeveiliging. Zie hiervoor [vu.nl](https://vu.nl) en specificeer:

- Het [Reglement verwerking persoonsgegevens medewerkers Vrije Universiteit Amsterdam](#)
- Het [Reglement ICT-voorzieningen voor medewerkers Vrije Universiteit Amsterdam](#)

Het niet naleven van instructies, zoals deze reglementen, kan arbeidsrechtelijke consequenties hebben.

### 3. Vragen?

Als je twijfelt of vragen hebt over privacy, neem dan contact op met de [Privacy Champion](#) van jouw Faculteit of Dienst. Zij helpen je graag verder.

Als je iets nieuws gaat doen waarbij (mogelijk) persoonsgegevens worden verwerkt, volg dan het Privacy Stappenplan ([zie bijlage bij dit document](#)). Daarin staat uitgelegd welke stappen je in ieder geval moet zetten.

*Let op: binnen een Faculteit of Dienst kunnen aanvullend specifieke procedures en afspraken gelden voor privacy en gegevensbescherming.*

Daarnaast zijn er nog een aantal andere collega's en loketten die je kunnen helpen:

- Als je vragen hebt over research data management kun je terecht bij de [RDM-supportdesk](#).
- Heb je hulp nodig bij valorisatie, neem dan contact op met [IXA](#).
- Heb je hulp nodig bij een kwestie omtrent onderzoeksubsidie, neem dan contact op met de [Subsidiedesk](#).
- Heb je specifieke juridische vragen, dan kun je terecht bij [Bestuurlijke en Juridische Zaken](#).
- Is er iets misgegaan en/of vermoed je een [datalek](#)? Neem dan z.s.m. contact op met de [IT-servicedesk](#).
- Heb je een klacht m.b.t. privacy? Dan kun je terecht bij de interne toezichthouder, de [Functionaris Gegevensbescherming](#).
- Voor meer informatie over privacy kun je ook de [handleiding van de Rijksoverheid](#) lezen of de website van de [Autoriteit Persoonsgegevens](#) raadplegen.