Medewerkershandboek AVG in de praktijk

1. Inleiding

Per 25 mei 2018 geldt de nieuwe Europese privacywet de “Algemene Verordening Gegevensbescherming” (AVG) . Dit betekent dat Persoonsgegevens van studenten, medewerkers, relaties en onderzoekdeelnemers nog zorgvuldiger dan voorheen behandeld moeten worden. Het kernwoord uit de AVG is “**beperk**”.

- Beperk het aantal personen van wie Persoonsgegevens worden verzameld en de hoeveelheid Persoonsgegevens die per persoon worden verzameld en verwerkt.
- Beperk het aantal personen dat toegang heeft tot deze Persoonsgegevens (autorisatie).
- Beperk het risico dat Persoonsgegevens onrechtmatig gedeeld worden met derden (zo nodig: verwerkersovereenkomsten).
- Beperk het risico dat Persoonsgegevens beschikbaar komen voor onbevoegden (datalekken).

Wellicht een overbodige opmerking: de AVG politieagent is niet de FG van de Open Universiteit (OU) of de Privacy officer of de leidinggevenden, maar dat zijn onze studenten, medewerkers, relaties en onderzoekdeelnemers die hun rechten opeisen. Zij kunnen ook een klacht indienden over, bijvoorbeeld, een bepaalde Verwerking of een ontbrekende verwerkersovereenkomst.

1.1 Informatiebronnen

Informatie voor medewerkers over *Informatiebeveiliging en Privacy* staat op onze intranetsite (Startpagina intranet → ICT → Informatiebeveiliging en privacy). Die webpagina bevat:

- Dit handboek: het beschrijft een aantal aandachtspunten in verband met privacy waar alle medewerkers van de Open Universiteit sinds 25 mei 2018 rekening mee moeten houden.
- Het vastgestelde *Informatiebeveiligings- en privacy beleid* van de OU.
- Aanvullende informatie over wat van medewerkers wordt verwacht op het gebied van Informatiebeveiliging en privacy.
- Werkinstructies (voor zover beschikbaar) om te zorgen dat de Open Universiteit aan de AVG voldoet.

Op onze openbare website www.ou.nl/privacy zijn beleidsdocumenten en dataregisters – inclusief leeswijzer – in te zien en te downloaden.

1.2 Begrippenlijst

Waar de onderstaande begrippen (of hun meervoudsvorm) in dit handboek met een hoofletter worden geschreven, wordt de hier gegeven omschrijving bedoeld.

Begrip	**Omschrijving**
Betrokkene	Iemand van wie Persoonsgegevens worden verwerkt. De Open Universiteit onderscheidt vier categorieën van Betrokkenen namelijk: studenten, medewerkers, relaties en onderzoekdeelnemers.
Functionaris voor de gegevensbescherming (FG)	Houdt binnen de OU toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling. Het CvB heeft een van de Juridisch adviseurs benoemd in de rol van FG. Contact via: FG@OU.nl

Begrip	Omschrijving
Persoonsgegeven	Alle informatie waarmee een persoon direct of indirect geïdentificeerd kan worden. Niet alleen iemands naam, adres en woonplaats zijn Persoonsgegevens, maar bijvoorbeeld ook telefoonnummers, mailadressen, foto's of studieresultaten vallen hieronder. Burger Service Nummers (BSN) en gegevens over bijvoorbeeld iemands ras, godsdienst, vakbondslidmaatschap of gezondheid worden bijzondere Persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd. Op verwerkingen waarin geen Persoonsgegevens zijn opgenomen, is de AVG niet van toepassing.
Privacy officer (PO)	Een rol op strategisch en tactisch niveau. De Privacy officer heeft direct toegang tot de verantwoordelijken voor de Persoonsgegevens maar is zelf geen lijnverantwoordelijke. Hij adviseert die verantwoordelijken m.b.t. de Verwerking van Persoonsgegevens binnen de kaders van de AVG. De Privacy officer ondersteunt de FG bij dienst taken maar heeft niet de bevoegdheden van de FG. Contact via: privacyofficer@OU.nl
Servicedesk	Loket voor alle ondersteunende (ICT-)diensten van de OU. Contact via Servicedesk@OU.nl, 045-5762306.
Verwerking	Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, kopiëren, bijwerken, afschermen, wissen of vernietigen van gegevens.
Verwerker	Een door OU ingeschakelde (derde) partij die ten behoeve van OU en op basis van diens schriftelijke instructies, Persoonsgegevens verwerkt.
Verwerkingsverantwoordelijke	College van bestuur van OU die het doel en de middelen van de Verwerking van Persoonsgegevens vaststelt.

2. Rechten van Betrokkenen

De rechten van de Betrokkenen (studenten, medewerkers, relaties en onderzoekdeelnemers) zijn verankerd in de AVG. Betrokkenen kunnen onder andere inzage, correctie of verwijdering van hun Persoonsgegevens uit de systemen eisen. De OU heeft georganiseerd dat Betrokkenen van deze rechten gebruik kunnen maken, o.a. door de medewerkers van SenI te instrueren hoe dergelijke verzoeken moeten worden behandeld. De rechten van Betrokkenen gelden niet per definitie voor Persoonsgegevens die als persoonlijke aantekening of correspondentie van een medewerker kunnen worden beschouwd.

De Open Universiteit beschouwt documenten die niet met anderen worden gedeeld als persoonlijke aantekeningen. Indien je bijvoorbeeld een Word-document met Persoonsgegevens op de M-drive bewaart zijn de rechten van de Betrokkenen daarop niet per definitie van toepassing. Ook e-mailberichten die slechts gedeeld zijn met een relevante doelgroep, kunnen in veel gevallen gezien worden als persoonlijke correspondentie. De eerder genoemde **beperk**ingen blijven hier gewoon van kracht: Indien een Betrokkene aangeeft van bovengenoemde rechten gebruik te willen maken, neem dan contact op met de Privacy officer.

Het spreekt voor zich dat (studie)adviezen aan studenten e.d. niet onder persoonlijke aantekeningen vallen.

3. Verwerkingsdoel en grondslagen

Voor het rechtmatig verwerken van Persoonsgegevens moeten een verwerkingsdoel en een verwerkingsgrondslag zijn vastgesteld. De eerste vraag die je stelt bij het beginnen met een nieuwe Verwerking is: "**w**elke Persoonsgegevens van **w**ie ga ik verzamelen en voor **w**elk doel heb ik die nodig". Je moet dus het doel en de noodzaak van het verzamelen van elk van die Persoonsgegevens kunnen onderbouwen. Denk daarbij aan wat eerder in dit handboek werd gesteld over **beperk**.

Als er Persoonsgegevens worden verwerkt, moet de tweede vraag gesteld worden: "Is er een grondslag?". Met andere woorden: 'Mogen we die Persoonsgegevens verwerken?' Voor de duidelijkheid: voor alle Persoonsgegevens die wij vragen moet een grondslag zijn vastgesteld.

De mogelijke grondslagen zijn:

W Wettelijke verplichting: De OU is wettelijk verplicht om deze Persoonsgegevens te verwerken (Bijvoorbeeld: de verplichting van de OU om informatie over studenten te verstrekken aan DUO en informatie over medewerker aan Belastingdienst en Pensioenfonds).

O Overeenkomst: De OU moet deze Persoonsgegevens verwerken om een overeenkomst waarbij Betrokkene partij is, te kunnen uitvoeren. Zulke overeenkomsten zijn bijvoorbeeld: de Inschrijving van een student of de aanstelling van een medewerker.

Gb Gerechtvaardigd belang: De OU heeft er een gerechtvaardigd belang bij om bepaalde verwerkingen van Persoonsgegevens uit te voeren (bijvoorbeeld voor het voeren van een Studentenadministratie of een Personeelsadministratie).

T Toestemming: de Betrokkene (student, medewerker of relatie) heeft aantoonbaar zijn ondubbelzinnige toestemming gegeven voor de Verwerking van zijn Persoonsgegevens voor een of meer specifieke doelen (Bijvoorbeeld: deelname aan wetenschappelijk onderzoek of het gebruik van zijn foto op een website).

V Vitaal belang: De OU verwerkt deze Persoonsgegevens omdat daar een vitaal belang van de Betrokkene mee gediend is (Bijvoorbeeld: Persoonsgegevens die nodig zijn om bij een levensbedreigende situatie adequaat te kunnen ingrijpen).

Ab Algemeen belang: De OU verwerkt deze Persoonsgegevens om taken van algemeen belang te kunnen uitvoeren (Bijvoorbeeld: Onderwijs en Onderzoek).

Als er geen grondslag is, of de grondslag is (nog) niet bekend, neem dan contact op met de Privacy officer alvorens te beginnen met het verzamelen van Persoonsgegevens.

4. Voorkomen van onrechtmatige Verwerking van Persoonsgegevens

Als we vervolgens Persoonsgegevens rechtmatig verwerken met een duidelijk doel en een vastgestelde grondslag, is het zaak te voorkomen dat die Persoonsgegevens daarnaast ook nog onrechtmatig worden verwerkt. We onderscheiden daarvoor 3 scenarios:

- Voorkomen van onrechtmatige Verwerking binnen de OU.
- Voorkomen van bedoelde maar onrechtmatige Verwerking buiten de OU.
- Voorkomen van onbedoelde onrechtmatige Verwerking buiten de OU.

4.1 Voorkomen van onrechtmatige Verwerking binnen de OU

Ook binnen de OU moet de toegang tot Persoonsgegevens tot het noodzakelijke worden **beperk**t.

- Geef alleen toegang aan medewerkers die de Persoonsgegevens nodig hebben voor hun OU werkzaamheden.
- Geef die medewerkers niet meer toegangsrechten dan ze daarvoor nodig hebben (geen schrijfrechten als leesrechten volstaan).
- Spreek met die medewerkers af dat ze geen eigen kopieen van die Persoonsgegevens maken of richt de toegang zo in dat ze dat niet kunnen.
- Deel geen Persoonsgegevens via e-mail, ook niet met OU collega's. Zie hoofdstuk 6.3 Veilige uitwisseling van Persoonsgegevens en andere vertrouwelijke informatie voor alternatieven.

4.2 Voorkomen van bedoelde maar onrechtmatige Verwerking buiten de OU

De OU blijft verantwoordelijk voor de Persoonsgegevens die zij verwerkt, ook als ze die gegevens met anderen deelt; zij blijft dus Verwerkingsverantwoordelijke! Om Persoonsgegevens rechtmatig te kunnen delen, is er altijd een overeenkomst nodig tussen de OU en de partij met wie zij de Persoonsgegevens deelt. In zo'n overeenkomst wordt bijvoorbeeld geregeld wat de andere partij met de gegevens mag doen en wie waarvoor verantwoordelijk is. Als zo'n overeenkomst er niet is, dan mogen de Persoonsgegevens niet gedeeld worden en is de Verwerking onrechtmatig.

We onderscheiden twee soorten delen van Persoonsgegevens:

- De OU als Verwerkingsverantwoordelijke schakelt een externe Verwerker in om in opdracht van de OU Persoonsgegevens te verwerken.
- De OU verstrekt Persoonsgegevens aan een andere partij en die partij wordt dan zelf Verwerkingsverantwoordelijke.

Neem in beide gevallen contact op met de Privacy officer om te overleggen of de Persoonsgegevens gedeeld kunnen worden en wat daarvoor moet worden gedaan.

4.2.1 Verwerkersovereenkomst

Indien Persoonsgegevens waarvoor de OU de Verwerkingsverantwoordelijke is in opdracht van de OU buiten de OU worden verwerkt, dan dienen hierover afspraken te worden gemaakt met de Verwerker. De afspraken met de verwerker dienen (voor elke leverancier/elk product apart) vastgelegd te worden in een verwerkersovereenkomst.

Als je een nieuwe dienst of applicatie wilt gebruiken[1], zorg dan dat dit wordt aangevraagd via de Servicedesk. Zij gaan via de Privacy officer na of er een verwerkersovereenkomst nodig is. Zo ja, dan is de aanvrager verantwoordelijk voor het (doen) afsluiten van een verwerkersovereenkomst. De Privacy officer ziet er op toe dat de verwerkersovereenkomsten procedure correct doorlopen wordt.

Ook als studenten zich in het kader van hun studie bij de OU zelf (aan)melden bij een leverancier die hun Persoonsgegevens verwerkt, moet de OU een verwerkersovereenkomst met die leverancier (=Verwerker) afsluiten. Cruciaal is de vraag: “Zou de student deze dienst hebben afgenomen als hij/zij niet studeerde aan de OU?”. Als het antwoord ‘nee’ is, dan moet er een verwerkersovereenkomst worden afgesloten.

Bij de Verwerking van Persoonsgegevens door een externe Verwerker, moet er altijd een verwerkersovereenkomst zijn. Als een Verwerker niet bereid is om een verwerkersovereenkomst af te sluiten, dan stopt de samenwerking.

4.2.2 Overeenkomst tussen twee Verwerkingsverantwoordelijken

Op het moment dat je op eigen initiatief Persoonsgegevens zou willen delen buiten de OU, vraag dan altijd eerst de Privacy officer om advies.

Medewerkers van de OU mogen Persoonsgegevens alleen delen met andere Verwerkingsverantwoordelijken als daar een grondslag voor is. Anders is het verstrekken van Persoonsgegevens niet toegestaan. Wanneer je een verzoek krijgt voor het verstrekken van Persoonsgegevens aan een partij buiten de OU, vraag de aanvrager dan om door de FG van zijn organisatie de grondslag bij het verzoek te laten aanleveren. De Privacy officer van de OU kan dan beoordelen of dit verzoek gehonoreerd kan worden. Daarbij wordt ook bepaald of daartoe een nieuwe overeenkomst moet worden afgesloten.

4.3 Voorkomen van onbedoelde onrechtmatige Verwerking buiten de OU

Door fouten of informatiebeveiligingsincidenten kunnen Persoonsgegevens onbedoeld in handen vallen van personen of organisaties welke die Persoonsgegevens niet mogen verwerken. In dat geval is de OU jegens Betrokkenen verantwoordelijk voor het feit dat hun Persoonsgegevens onrechtmatig (kunnen) worden verwerkt. Onrechtmatige Verwerking van Persoonsgegevens kan niet worden hersteld, dus moet onze energie zijn gericht op het voorkomen daarvan. De AVG schrijft ook voor dat organisaties passende ‘technische en organisatorische maatregelen’ moeten nemen om Persoonsgegevens te beschermen.

Als niet kan worden uitgesloten dat Persoonsgegevens onrechtmatig worden verwerkt, is er sprake van een datalek. Als je vermoedt dat er een datalek heeft plaatsgevonden, meld dat dan meteen bij de Servicedesk (servicedesk@ou.nl, telefoon: 045-576 2306). De procedure die dan gestart wordt, is beschreven in het Ict ABC: *Meldplicht datalekken*. Als deel van die procedure maakt onze FG de afweging of het datalek gemeld moet worden bij de Nederlandse toezichthouder op de AVG: de Autoriteit Persoonsgegevens.

Voorbeelden van datalekken zijn:

[1] Dat geldt dus ook voor diensten in de cloud die “met één click” gratis worden aangeboden.

- Verlies van een onversleutelde mobiele gegevensdrager (bijvoorbeeld usb-stick, laptop, smartphone of tablet) als hier Persoonsgegevens op staan.
- Verlies van een smartphone, omdat deze – naast zijn rol als gegevensdrager – ook toegang geeft tot informatie waaronder bijvoorbeeld: werk e-mail, notities, automatische inlog in systemen.
- Een computer thuis, die gehackt of gestolen wordt en waarop b.v. een Excel bestand met Persoonsgegevens staat.
- E-mail met Persoonsgegevens, zeker als die is verstuurd naar de verkeerde persoon.
- 'Offline' of 'papieren' datalekken; denk hierbij aan printjes in de papierbak, lijsten met Persoonsgegevens onbeheerd op het bureau, dossiers in een gestolen tas.

Zie hoofdstuk 6 Praktische handreikingen voor mogelijkeden om datalekken te voorkomen.

5. Wetenschappelijk onderzoek

Onderstaand volgen enkele hoofdpunten die – aanvullend op het voorafgaande – richtinggevend zijn voor het verwerken van Persoonsgegevens in onderzoek. Verdere aanscherping kan en dient nog plaats te vinden op basis van verdere nationale en internationale consensusvorming. Zo wordt de gedragscode Persoonsgegevens van de VSNU momenteel nog herzien. Bij onduidelijkheid of vragen over de gevolgen van de AVG voor het wetenschappelijk onderzoek, is het mogelijk contact op te nemen met de Privacy officer.

- De grondslag voor de Verwerking van Persoonsgegevens ten behoeve van wetenschappelijk onderzoek is **T**oestemming. De onderzoekdeelnemer dient vooraf voldoende geïnformeerd te zijn (via een informatiebrief) en specifiek en ondubbelzinnig toestemming te verlenen voor de verzameling en Verwerking van zijn of haar Persoonsgegevens (via een toestemmingsverklaring/Informed Consent).
- Voor onderzoekers is er geen apart dataregister, ze zijn immers "medewerkers in loondienst" of "medewerkers niet in loondienst" of "relaties".
- Voor onderzoekdeelnemers is er geen dataregister. Indien er persoonsgegevens worden verwerkt, dient informatie over deze verwerking in de informatiebrief opgenomen te zijn. Voor meer informatie zijn ook de websites van de commissie Ethische Toetsing Onderzoek (cETO) en de Centrale Commissie Mensgebonden Onderzoek (CCMO) te raadplegen. Een format voor de informatiebrief is te downloaden via deze link.
- Onderzoekdeelnemers hebben het recht op inzage, of om te eisen dat hun persoonsgegevens worden gewijzigd of niet meer worden verwerkt en verwijderd dienen te worden De rechten van de betrokkenen kunnen worden beperkt indien deze de doeleinden van het onderzoek belemmeren. Op het moment dat een deelnemer een beroep doet op het recht van de betrokkenen, neem dan contact op met de Privacy officer.
- Indien persoonsgegevens worden verwerkt in het kader van onderzoek dan geldt er een bewaartermijn van 10 jaar voor niet-medisch onderzoek en een bewaartermijn van 15 jaar voor medisch onderzoek.
- Onderzoeksgegevens dienen waar mogelijk gepseudonimiseerd te worden. Dat wil zeggen dat alle informatie waarmee een betrokkene direct of indirect geïdentificeerd kan worden in de onderzoeksgegevens wordt vervangen door codes die alleen door daartoe geautoriseerde onderzoekers tot de persoonsgegevens kunnen worden herleid. Dat herleiden dient voor zo min mogelijk onderzoekers – denk aan 3 onderzoekers die alleen op persoonlijke titel toegang hebben – mogelijk te zijn. Het loggen van dit proces is wenselijk, zodat daarover zo nodig verantwoording kan worden afgelegd. Uitsluitend indien dit niet in strijd is met de wetenschappelijke integriteit, is het mogelijk om de onderzoeksgegevens te anonimiseren. Dat wil zeggen dat de onderzoeksgegevens zo worden verwerkt dat deze op geen enkele manier herleidbaar zijn tot de betrokkenen.

6. Praktische handreikingen

6.1 Wet- en regelgeving over informatiebeveiliging

- Wees je bewust van bijzondere Persoonsgegevens. Dergelijke gegevens vereisen extra waakzaamheid en mogen alleen onder strenge voorwaarden worden verwerkt en gedeeld. Bijvoorbeeld een foto van studenten plaatsen op social media of het cv van een sollicitant aan een collega doorsturen mag alleen onder voorwaarden (grondslag: Toestemming);
- Heb je het vermoeden dat er op enige wijze misbruik gemaakt wordt van de ICT-voorzieningen, meldt dit dan bij cert@ou.nl. Meldingen worden discreet behandeld.

6.2 Veilig bewaren van Persoonsgegevens en andere vertrouwelijke informatie

Wees je bewust van de risico's van vertrouwelijke bestanden die lokaal zijn opgeslagen. Ga zorgvuldig om met je mobiele apparaten en voorkom diefstal.

- Bewaar geen vertrouwelijke bestanden lokaal op je onversleutelde laptop. Als je die verliest dan kan de "vinder" de harde schijf eruit halen en alle documenten lezen. Zie 6.7 Veiligheid van gegevensdragers
- Gebruik voor het bewaren van Persoonsgegevens en andere vertrouwelijke informatie geen cloud diensten (Dropbox, Google drive, iCloud, etc.) waarmee de OU geen verwerkersovereenkomst heeft afgesloten.

  Bij het gebruik van Apple apparatuur is enig gebruik van iCloud voor bijvoorbeeld synchronisatie vrijwel onvermijdelijk. Zorg dan in ieder geval dat er geen informatie van de OU in die iCloud terecht komt.

  SURFdrive is een goed alternatief. Als je nog geen toegang tot SURFdrive hebt, kun je die aanvragen bij de Servicedesk.
- Zie in het Ict ABC: *Veilig bewaren van informatie*.

6.3 Veilige uitwisseling van Persoonsgegevens en andere vertrouwelijke informatie

Verstuur nooit vertrouwelijke informatie onversleuteld via e-mail, ook niet aan een OU collega op haar OU e-mailadres. Alternatieven in afnemende volgorde van wenselijkheid:

- In het ATI-proces is een zogenaamde Berichtenbox geïmplementeerd waarmee – vanuit administratieve processen van de OU – op een veilige manier documenten aan studenten kunnen worden aangeboden. Dit is eenrichtingsverkeer: van de OU naar de student.
- De onderwijs gebonden uitwisselfaciliteit binnen yOUlearn zijn voor die toepassing een geschikt alternatief. Deze faciliteit ondersteunt tweerichtingsverkeer tussen studenten en docenten.
- Verstuur overige vertrouwelijke informatie naar en tussen studenten, medewerkers en derden via de SURF dienst Filesender (Ict ABC: *Filesender*) en gebruik de optie File Encryption. Deze methode werkt ook voor grote bestanden en voor personen die zelf geen toegang hebben tot Filesender.
- Plaats de vertrouwelijke informatie in een Word document dat je als attachment aan de e-mail mee stuurt. Voorzie dat vertrouwelijke Word documenten van een wachtwoord. Zie in het Ict ABC: *Versleutelen van Word en Excel bestanden*. Daar is ook beschreven hoe je het wachtwoord veilig bij de ontvanger krijgt.

6.4 Fysieke beveiliging

- Vergrendel het scherm van je computer zodra je die ergens (ook op je eigen werkplek) achterlaat, zelfs als je maar even weg bent. Met de toetsen <windowstoets+L> voor Windows of <ctrl-⌘+Q> voor macOS zet je jouw computer snel op slot (locken). Je voorkomt hiermee dat iemand onder jouw gebruikersnaam acties gaat uitvoeren.

- Papieren documenten met gevoelige informatie, zoals Persoonsgegevens, mogen niet openbaar worden. Laat die documenten dus niet onbeheerd achter, op je bureau, bij de printer of waar dan ook. Op de campus in Heerlen staan speciale afgesloten papiercontainers voor vertrouwelijk papier. In andere gevallen moet het papier na gebruik versnipperd worden. Anders kan de informatie misbruikt worden en ook dan is er sprake van een datalek.
- Controleer op kantoor altijd de identiteit van personen zonder OU-badge die je niet kent. Vraag gerust aan een onbekende wie hij/zij is en wat hij/zij komt doen. Deze persoon zou namelijk kwade bedoelingen kunnen hebben. Iedereen vindt het fijn om in een veilige omgeving te werken, dus de bonafide gast heeft er geen moeite mee dat jij deze vragen stelt.

6.5 Veilig gebruik van e-mail en internet

- Gebruik nooit openbare wifi-netwerken voor het versturen van Persoonsgegevens en andere vertrouwelijke informatie: alles wat je doet kan afgeluisterd en zelfs aangepast worden.
- Klik niet op een link in een phishing mail. Heb je een phishing mail ontvangen en de link per ongeluk toch aangeklikt, meldt dit dan bij de Servicedesk zodat anderen gewaarschuwd kunnen worden en de gevolgen beperkt worden.
- Ben alert op bestandstypen van attachments. Het is niet logisch als je een executable (.exe) bestand ontvangt terwijl je een Word-bestand (.docx) verwacht.

6.6 Veilige wachtwoorden

- Gebruik lange wachtwoorden; wachtwoordzinnen zijn het gemakkelijkst te onthouden. Deze wachtwoorden zijn lastig te kraken door zogenaamde ‘brute-force’ aanvallen, waarbij alle mogelijke combinaties van tekens worden uitgeprobeerd.
- Schrijf je gebruikersnaam en wachtwoord niet op dezelfde plek op. Als het document waarop beide staan gevonden wordt, dan hebben criminelen direct toegang tot jouw account. NB: Omdat je OU gebruikersnaam bij veel mensen bekend kan zijn, is het opschrijven van je wachtwoord extra gevaarlijk.

  Daarom is het zinvol om gebruik te maken van een wachtwoordmanager. Op deze wijze kan je op een makkelijke manier gebruik maken van sterke wachtwoorden die jij niet zelf hoeft te onthouden, dat doet namelijk de wachtwoordmanager voor jou. Zie voor Windows laptops in het ICT ABC: Wachtwoorden bewaren met Keepass. Gebruikers van clients met macOS kunnen de applicatie Sleutelhanger gebruiken, maar daarvan is nog geen documentatie beschikbaar in het ICT ABC.
- Geef je wachtwoord nooit aan anderen (dus ook niet aan collega’s van je afdeling of secretaresses);
- Gebruik voor ieder account een ander wachtwoord. Mocht één wachtwoord uitlekken dan heeft de misbruiker niet direct toegang tot andere accounts;
- Maak voor toegang tot gevoelige informatie – indien mogelijk – gebruik van aanvullende authenticatie middels two factor authentication (2FA). GSO zoekt nog naar mogelijkheden om deze faciliteit voor alle medewerkers beschikbaar te stellen.

6.7 Veiligheid van gegevensdragers

- Als je vertrouwelijke gegevens bewaart op een mobiel device, zorg dan dat de gegevensopslag daarvan versleuteld is. iOS apparatuur (iPhone, iPad) is standaard versleuteld. GSO levert momenteel Windows 10 laptops standaard uit met versleutelde opslag. Er zijn nog geen faciliteiten om de opslag van oudere laptops alsnog te laten versleutelen.
- Het bovenstaande geldt ook voor de externe gegevensdragers USB-stick of USB-schijf. Gebruik je toch een externe gegevensdrager, zorg er dan voor dat de gegevensdrager versleuteld is. Zie voor Windows laptops in het ICT ABC: Versleutelen verwisselbare (USB) schijven voor BV6 en Versleutelen verwisselbare (USB) schijven voor BV10.

- Als gegevens op een gegevensdrager niet versleuteld zijn, dan is dit geen veilige plaats om Persoonsgegevens op te slaan. Mocht je een onversleutelde gegevensdrager met Persoonsgegevens kwijtraken, dan is er sprake van een datalek. Meld dit direct bij de Servicedesk.
- Gevonden gegevensdragers (zoals usb-sticks) zijn niet veilig. Steek ze dus niet zomaar in een computer. Als er een virus op een usb-stick staat, is het veelal reeds schadelijk als de gebruiker deze in zijn of haar computer steekt, dus zelfs zonder dat bestanden expliciet worden geopend.

6.8 Veilig gebruik van formulieren

Formulieren worden vaak gebruikt om gegevens van klanten, studenten of onderzoeksdeelnemers te verzamelen. Dan verwerk je persoonsgegevens en moet je rekening houden met de Privacy wetgeving (AVG).

De persoon die het formulier opstelt (de maker) is verantwoordelijk voor het voldoen aan de AVG:

- De maker bepaalt welke persoonsgegevens hij verzamelt en moet dus voor alle verzamelde gegevens een grondslag en een doel kunnen aangeven.
- De maker bepaalt welke maatregelen moeten worden getroffen om de persoonsgegevens in het formulier adequaat te beschermen tegen onrechtmatige verwerking. Die maatregelen moeten in overeenstemming zijn met het risico voor de privacy van de betrokkene. Hoe meer en hoe gevoeliger gegevens worden verzameld, hoe groter het risico voor de privacy van de betrokkene en dus hoe sterker de maatregelen die getroffen moeten worden.

Vraag voor een nieuw formulier, dus een nieuwe verwerking van persoonsgegevens, altijd advies aan de Privacy officer van de OU.

De maker moet er namens de OU voor zorgen dat de juiste maatregelen worden getroffen. Dat kan alleen als het formulier op de ICT-infrastructuur van de OU wordt gehost of op de ICT-infrastructuur van een leverancier waarmee de OU een verwerkersovereenkomst heeft afgesloten. **NB:** Niet elke leverancier is bereid en in staat om de juiste maatregelen te treffen voor de verwerking van persoonsgegevens met een hoog risico!

Als je op een formulier alleen gesloten vragen aanbiedt, dan heb je precies in de hand welke persoonsgegevens er worden verwerkt. Bij open vragen met een invulveld is dat veel minder het geval. De respondent kan daar heel andere informatie invullen dan de maker bedoelde, waardoor het risico voor de privacy van de betrokkene groter kan worden dan waar de maker rekening mee hield. Het feit dat de betrokkenen zelf, vrijwillig, deze ongevraagde privacygevoelige informatie verstrekte, doet niet af aan de verantwoordelijkheid van de OU c.q. de maker.

Probeer dus het gebruik van open vragen met invulvelden te vermijden. Als open vragen onvermijdelijk zijn, neem dan in het formulier bij ieder veld een toelichtende tekst op waarin je aangeeft dat hier geen gevoelige persoonsgegevens mogen worden ingevuld. Vermeldt hier tevens de grondslag (zie §3) en het doel van de opgevraagde informatie; dit kan heel summier zijn. Biedt de toelichtende tekst bijvoorbeeld aan middels een *[?]* symbool na het invulveld, zodat de respondent op dat symbool kan klikken om de toelichting te lezen.

Voorbeelden:

- Vooropleiding [?] Noem hier alleen de afgesloten vooropleidingen. Als u informatie wilt delen over niet afgesloten opleidingen en de reden van dat niet afsluiten, kruis dan het vak *Neem telefonisch contact met mij op* aan. Wij vragen naar uw vooropleiding om beter te kunnen beoordelen welke vervolgopleiding het meest passend voor u is. Onze grondslag voor het verwerken van dit gegeven is Uitvoering van de onderwijsovereenkomst.
- Voor- en achternaam [?] Wij vragen dit om onze correspondentie persoonlijk te kunnen maken. Onze grondslag voor de verwerking van dit gegeven is Uitvoering van de onderwijsovereenkomst.