Open Universiteit

Introductie

Algemene Verordening Gegevensbescherming

Nieuwe medewerkers van de Open Universiteit

De Algemene Verordening Gegevensbescherming

- Per 25 mei 2018 is de AVG definitief in werking getreden. De AVG is een Europese verordening en is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in alle EU-landen. Deze EU-verordening geldt wereldwijd voor alle organisaties en ondernemingen die persoonsgegevens bijhouden en verwerken van EU-burgers.
- In de AVG zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd.
- In Nederland wordt de AVG gehandhaafd door de Autoriteit Persoonsgegevens (AP).
- Iedere medewerker van de OU werkt met (persoons)gegevens. Voor de OU is het belangrijk dat medewerkers de juiste gegevens delen met de juiste mensen. Daar dragen we samen verantwoordelijkheid voor.

Grondslagen en uitganspunten

Grondslag voor de verwerking van persoonsgegevens (art. 6 AVG)

1. Toestemming van betrokkene
2. Noodzakelijk voor de uitvoering van een overeenkomst
3. Wettelijke verplichting
4. Vitale belangen van de betrokkene of van een andere natuurlijke persoon beschermen
5. Taak van algemeen belang of openbaar gezag
6. Gerechtvaardigde belang

Uitgangspunten inzake verwerking van persoonsgegevens (art. 5 AVG)

1. Rechtmatigheid, behoorlijkheid en transparantie
2. Doelbinding
3. Minimale gegevensverwerking
4. Juistheid
5. Opslagbeperking
6. Integriteit en vertrouwelijkheid
7. (Verantwoordingsplicht)

Verwerking van Persoonsgegevens

Verwerken van persoonsgegevens houdt in: alles wat een organisatie met persoonsgegevens kan doen, van verzamelen tot en met vernietigen:

“Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.”

Persoonsgegevens

- Alle informatie die direct over iemand gaat, ofwel naar deze persoon te herleiden is, merken we aan als een persoonsgegeven. Er is sprake van herleidbare persoonsgegevens, wanneer gegevens die in combinatie met andere gegevens iets zeggen over een persoon.
    - Er zijn veel soorten (herleidbare) persoonsgegevens. Voorbeelden zijn iemands naam, adres, woonplaats, kenteken, IP-adres, haarkleur, tentamenresultaat, studentnummer, telefoonnummers en postcodes met huisnummers.
    - Bijzondere en/of gevoelige gegevens als iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid worden aangemerkt als bijzondere persoonsgegevens. Deze worden door de wetgever extra beschermd.
- De AVG is van toepassing op gepseudonimiseerde gegevens. De AVG is niet van toepassing op geanonimiseerde gegevens. Toch mag niet te snel worden aangenomen dat persoonsgegevens zijn geanonimiseerd. Een dataset die op zichzelf volledig geanonimiseerd lijkt, kan (al dan niet in combinatie met een andere dataset) toch gegevens bevatten die te herleiden zijn tot bepaalde individuen.

Ik ga persoonsgegevens verwerken, waar moet ik op letten?

- Ga je persoonsgegevens verwerken, vraag je dan af of je de verwerking kunt baseren op een van de wettelijke grondslagen.
- Kun je de verwerking baseren op basis van een wettelijke grondslag, zorg dan dat je de uitgangspunten van de AVG in acht neemt.
- Laat je gegevens verwerken door een andere partij, dan moet mogelijk een verwerkersovereenkomst gesloten worden.
- Ga je bijzondere persoonsgegevens verwerken of grote hoeveelheden persoonsgegevens, dan brengt dit meer risico met zich mee. Dat kan betekenen dat er een Data Protection Impact Assessment (DPIA) uitgevoerd moet worden.
- De OU is extra waakzaam bij de verwerking (doorgifte) van persoonsgegevens naar een land buiten de Europese Economische Ruimte (EER). Dat betekent dat er een Data Transfer Impact Assessment (DTIA) uitgevoerd moet worden.
- Contacteer bij vragen de Servicedesk@ou.nl of de Privacyofficer@ou.nl

Wie kan mij helpen?

- Ik wil graag een informatiebeveiligingsincident melden of heb vragen over het gebruik van tools: Servicedesk@ou.nl
- Ik wil graag een (potentieel) datalek melden: FG@ou.nl (Saskia van der Westen)
- Ik wil graag advies over de verwerking van persoonsgegevens, het al dan niet uitvoeren van een (pre-)DPIA, het sluiten van verwerkersovereenkomsten: Privacyofficer@ou.nl (Mark Adriolo)
- Ik wil graag advies over het veilig opslaan van onderzoeksdata: Datasteward@ou.nl (Mellanie Geijen)
- Ik wil graag advies over (informatie)beveiligingsmaatregelen: Servicedesk@ou.nl.
- Ik heb een algemene vraag en weet niet goed wie mij kan helpen: Servicedesk@ou.nl

Er gaat iets fout, wat nu?

- Volgens de AVG heeft iedereen het recht dat er zorgvuldig wordt omgesprongen met zijn/haar persoonsgegevens. Wanneer er sprake is van ongeoorloofde of onbedoelde toegang tot, maar ook het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens, spreken we over een datalek. Er zijn talloze gebeurtenissen die binnen deze categorie kunnen vallen. Denk bijvoorbeeld aan het versturen van een e-mail naar de verkeerde persoon of aan diefstal van een laptop, hetgeen mogelijk ook gevolgen heeft voor anderen en een datalek kan veroorzaken. Een datalek kan risico's opleveren voor de privacy van anderen. Vaak zit er geen kwade opzet achter een datalek, maar onjuist menselijk handelen kan grote gevolgen voor anderen.
- Denk je dat sprake is van een datalek, dan is het belangrijk om na ontdekking zo snel mogelijk te handelen, zodat mogelijke gevolgen van het datalek zo klein mogelijk kunnen worden gehouden. We vragen je dan ook om datalekken zo snel mogelijk te melden bij de Servicedesk@OU.nl. De Servicedesk@ou.nl onderzoekt de melding en informeert indien nodig de Chief Information Security Officer (Martin.Romijn@ou.nl) en/of de Functionaris Gegevensbescherming (FG@ou.nl).

Hoe herken ik een phishing e-mail?

Het is vaak erg moeilijk om valse e-mails te herkennen, vooral als het gaat om gerichte aanvallen. Hieronder vind je een aantal adviezen om mogelijke valse e-mails te herkennen.

- Controleer het adres van de afzender. Vaak is het gebruikte e-mailadres vaag of een afgeleide versie van een echte bedrijfsnaam of de naam van een instantie. Kijk goed naar de domeinnaam waarvan je de e-mail hebt ontvangen. De domeinnaam is te herkennen aan alles wat achter het @-teken in het e-mailadres staat.
- Links in nepmails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd of leiden je naar een valse website. Klik dus nooit zomaar op de links in een e-mail die je niet vertrouwt. Controleer het adres van de link door, zonder erop te klikken, de cursor van je muis op de link te zetten en te kijken welk adres er verschijnt. Vaak worden lange links verkort met diensten als bijvoorbeeld T.co, bit.ly en Goo.gl. Erg handig, maar voor jou als ontvanger erg belangrijk om hier waakzaam op te zijn aangezien het lastig is om te achterhalen waar je nu precies op klikt en naar toe wordt geleid.
- Een bijlage in een nepmail kan ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Open dus nooit zomaar een bijlage van een e-mail die je niet vertrouwt.
- Vertrouw je een mail niet, meld je bij de Servicedesk.

Open Universiteit

BEDANKT VOOR JOUW AANDACHT

WWW.OU.NL