

AVG & onderzoek

Een handreiking voor het omgaan met de Algemene Verordening Gegevensbescherming bij onderzoek.



Mariëlle Rosendaal



HOGESCHOOL
HRM EN
PSYCHOLOGIE

AVG & onderzoek

*Een handreiking voor het omgaan met de Algemene
Verordening Gegevensbescherming bij onderzoek binnen
Fontys Hogeschool HRM & Psychologie*

Colofon

Deze handreiking is opgesteld in opdracht van de lectoraten Mens & Technologie en Dynamische Talentinterventies van Fontys Hogeschool HRM en Psychologie en de dienst IT van Fontys Hogescholen. Mijn dank gaat uit naar iedereen die heeft meegedacht en meegewerkt aan deze handreiking, in het bijzonder naar Rebecca Flanderijn, Gisa de Jonge, Janienke Sturm, Marian Thunnissen en Ruben van Ess, allen van Fontys Hogescholen.

Auteur & Opmaak: *Mariëlle Rosendaal*
Datum: *Mei 2019*

Meer informatie:

[https://connect.fontys.nl/instituten/fhhrmenp/privacyavg/
Paginas/home.aspx](https://connect.fontys.nl/instituten/fhhrmenp/privacyavg/Paginas/home.aspx)

hrmenpAVG@fontys.nl

Voorwoord

Zoals je misschien wel meegekregen hebt, is sinds 25 mei 2018 de AVG – Algemene Verordening Gegevensbescherming, privacywetgeving - van toepassing. In deze wetgeving staan regels over de verwerking van persoonsgegevens.

Zoals je ook wel weet, wordt er binnen ons instituut onderzoek gedaan door onder andere studenten, docenten en de lectoraten. In deze onderzoeken worden vaak bewust of onbewust persoonsgegevens verzameld. Denk bijvoorbeeld aan demografische gegevens, zoals leeftijd, geslacht, functie, werkervaring, et cetera, beeld- en geluidsopnames of kwalitatieve gegevens die duidelijk naar een persoon verwijzen, zoals een verhaal van iemand die een heel bekend boek heeft geschreven en daar over vertelt.

Omdat we binnen deze onderzoeken vaak persoonsgegevens verzamelen en verwerken, is het belangrijk dat we ons bewust zijn van én voldoen aan de AVG. Om dat zo eenduidig en gemakkelijk mogelijk te maken, hebben we deze handreiking opgesteld. Hierin vind je een begrippenlijst met de belangrijkste begrippen in de AVG, een stappenplan met hoe je je onderzoek kan ontwerpen en inrichten om aan de AVG te voldoen, praktische tips en een template voor een toestemmingsverklaring voor je onderzoek.

Heb je vragen over dit document, over het toepassen van de AVG in jouw onderzoek of over hoe je bijvoorbeeld studenten kan adviseren over de AVG? Ben je niet zeker of jouw toestemmingsverklaring voldoet aan de AVG? Vind je het fijn als iemand even naar jouw onderzoeksopzet meekijkt in het kader van de AVG? Heb je andere

vragen over privacy? Neem dan gerust contact op met hremenpAVG@fontys.nl als het gaat om vragen over de AVG in onderzoek, of met hremenpfunctioneelbeheer@fontys.nl als het om algemenere vragen gaat, of bijvoorbeeld over software. Zij helpen je graag verder.

Veel leesplezier en natuurlijk veel succes met je onderzoek!



Inhoud

Belangrijke definities & begrippen	9
Stappenplan	15
<i>Stap 1: Onderzoeksopzet</i>	15
<i>Stap 2: Privacy by Design</i>	16
<i>Stap 3: Toestemming</i>	19
<i>Stap 4: Hergebruik</i>	20
<i>Stap 5: Veilige opslag</i>	23
<i>Stap 6: Verwijderen</i>	24
<i>Stap 7: Recht op vergetelheid</i>	27
<i>Stap 8: Recht op inzage gegevens</i>	28
<i>Stap 9: Datalek = melden</i>	31
Praktische tips	33
Veelgestelde vragen	39



Kathleen & William
June 12, 2009

MARCO

LOVE

LOVE

GARRISON

LOVE

WASHER
JUNE 12, 2009

LOVE

B♥K

LOVE

LOVE

LOVE

LOVE

LOVE

JENNA + LIA

Belangrijke definities & begrippen

In dit hoofdstuk maak je kennis met een aantal definities en begrippen die belangrijk zijn om te kennen, wanneer we het over de AVG hebben. Mocht je, na het lezen van deze handreiking, meer vragen hebben over bepaalde definities of begrippen, neem dan contact op met hrmenpAVG@fontys.nl, dan breiden wij de lijst uit.

AVG

De Algemene Verordening Gegevensbescherming is wetgeving over privacy die in heel de Europese Unie geldt. De Engelse naam van de AVG is de General Data Protection Regulation (GDPR). In Nederland kennen we daarbij de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). De AVG en de GDPR is dus hetzelfde. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp). In de AVG staan regels voor de verwerking van persoonsgegevens. De AVG is op 24 mei 2016 in werking getreden en vanaf 25 mei 2018 is deze van toepassing. Men is sindsdien aanspreekbaar op naleving en vanaf dat moment kunnen boetes worden opgelegd.

Persoonsgegevens

Persoonsgegevens zijn gegevens die tot een persoon terug te herleiden zijn. Heel duidelijk is natuurlijk de naam, of adresgegevens, maar bijvoorbeeld ook de combinatie leeftijd, geslacht en functie zijn persoonsgegevens. Als je uit (een set van) gegevens kunt afleiden om welke unieke persoon het gaat, dan heb je te maken met (een set van) persoonsgegevens.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken. Ook genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn bijzondere persoonsgegevens. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij er sprake is van een specifieke wettelijke uitzondering. Denk je dat het voor jouw onderzoek nodig is om bijzondere persoonsgegevens uit te vragen? Neem dan eerst contact op met

hrmenpAVG@fontys.nl of

hrmenpfunctioneelbeheer@fontys.nl. Zij kijken mee naar jouw situatie en bepalen eventuele vervolgstappen hierin.

BSN (burgerservicenummer)

Het BSN is een persoonsgegeven dat wordt behandeld als bijzonder persoonsgegeven. Je mag het BSN niet verwerken (dus niet bevragen, opslaan of gebruiken), tenzij je hier wettelijke grondslag voor hebt. Het advies is dan ook: vraag nooit naar het BSN van respondenten. Ook niet om dit als sleutel te gebruiken om de persoon aan een set data te koppelen (zie ook 'Gecodeerde of gepseudonimiseerde data').

Geanonimiseerde data

Data die op geen enkele manier terug te herleiden is naar een unieke persoon, noemen we geanonimiseerde data. Een voorbeeld daarvan is bijvoorbeeld een 'mannelijke

student HRM van 21 jaar'. Er zijn meerdere mannelijke, 21-jarige HRM studenten. We kunnen daarmee geen unieke persoon aanwijzen. Geanonimiseerde data vallen niet onder de AVG.

Gecodeerde of gepseudonimiseerde data

Data die middels een sleutel wel terug te herleiden zijn naar de specifieke persoon, worden gecodeerde of ookwel gepseudonimiseerde data genoemd. Die sleutel is datgene wat de data aan de respondent linkt, bijvoorbeeld 'respondent 1' in de dataset, waarbij in een ander document vastgelegd is dat respondent 1 Jan Pietersen is. Gepseudonimiseerde data vallen wel onder de AVG.

Two factor authentication (2FA)

2FA is een beveiligingsmethode waarmee je, naast het inloggen met een gebruikersnaam en wachtwoord, nog een tweede beveiligingslaag toevoegt, zoals bijvoorbeeld het invullen van een per SMS ontvangen code. Verschillende applicaties hebben hier (verschillende) mogelijkheden voor. We raden je aan om informatie over de mogelijkheden op te zoeken via de Fontys portal, via de website van de leverancier van de applicatie, of vraag de dienst IT om hulp.

Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens, afgekort als AP, is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Als er sprake is van een (potentieel) hoge impact- datalek (zoals hierboven beschreven), dan wordt deze gemeld bij de AP. Lees meer over de AP op hun website: <https://autoriteitpersoonsgegevens.nl>.

Functionaris Gegevensbescherming (FG)

De functionaris gegevensbescherming (de FG) heeft deskundige kennis van gegevensbeschermingswetgeving en –praktijken en staat de verwerkingsverantwoordelijke (of verwerker) bij met het toezicht op de (interne) naleving van de AVG. Dit doet de FG onafhankelijk, zelfs als deze in dienst is van de verwerkingsverantwoordelijke. Niet alle bedrijven hebben een FG nodig, maar gezien de taak en de omvang van Fontys en het soort persoonsgegevens dat Fontys verwerkt, zijn hier wel FG's aangesteld.

Datalek

Wanneer persoonsgegevens onbedoeld gewijzigd, vrijgekomen of vernietigd zijn of 'iets of iemand' heeft onbedoeld toegang tot persoonsgegevens gekregen, is er sprake van een datalek. Verschillende datalekken kunnen verschillende impact hebben op de bescherming van persoonsgegevens en op de 'persoonlijke levenssfeer van betrokkenen' (ondervindt iemand schade van het datalek?). Afhankelijk van de (potentiële) impact moet een datalek wel of niet bij de Autoriteit Persoonsgegevens (AP) gemeld worden. Er is een meldplicht voor ernstige datalekken, bij de AP en soms ook bij de betrokken personen. Binnen Fontys melden we datalekken altijd intern, waarna de FG en de privacy officers zelf onderzoek doen naar de impact en vervolgens besluiten of het lek al dan niet bij de AP gemeld moet worden.

Datalek melden

Binnen Fontys HRM en P melden we een datalek bij hremenpfunctioneelbeheer@fontys.nl, of via de website rechtstreeks bij Fontys. Er wordt dan verder gekeken naar de potentiële impact en of er inderdaad een melding van het datalek bij de AP gedaan wordt. Meld een datalek altijd **zo snel mogelijk** ('zonder onredelijke vertraging'), uiterlijk **24 uur na kennisname van het datalek**.



Stappenplan voor het voldoen aan de AVG binnen onderzoek

Stap 1: Onderzoeksopzet

Wanneer je je onderzoek opzet, bedenk je dan welke persoonlijke gegevens je nodig hebt om je onderzoeksvraag te beantwoorden.

Maak het niet te klein: uit voortschrijdend inzicht kan blijken dat bepaalde data ook nuttig of zelfs nodig waren geweest. Het kan bijvoorbeeld in een onderzoek naar studiemotivatie op het hbo, bij het analyseren van je data blijken dat het toch wel handig was geweest om onderscheid te maken in vooropleiding. Helaas!

Maar maak het ook niet te groot: van welke data weet je nu al zeker dat je die nooit gaat gebruiken? Doe je bijvoorbeeld onderzoek naar eenzaamheid onder studenten? Dan is het niet nodig om te weten hoeveel te studenten verdienen met hun bijbaantje.

Stap 2: Privacy by Design

Privacy by Design betekent dat je in het ontwerpen van je onderzoek al zoveel mogelijk privacy of anonimiteit te waarborgen.

Doe je kwantitatief onderzoek? Probeer dan je vragen zo te stellen, dat de data vanzelf al anoniem wordt. Denk bijvoorbeeld in schalen: salaris in Euro's 1500-2500, 2500-3500, 3500-4500, leeftijd in jaren 20-24, 25-29, 30-34, lengte in centimeters 150-159, 160-169, 170-179, et cetera. Op deze manier is al vrijwel niet terug te herleiden wie de respondent is.

Is het noodzakelijk om persoonsgegevens te verzamelen? Richt dan je onderzoeksomgeving (denk aan mapstructuren en dergelijke) zodanig in, dat je documenten met persoonsgegevens direct kunt herkennen en daardoor meteen de juiste gegevensbescherming in kunt zetten (denk aan wachtwoorden en toegangsbeheer).

Houdt bij het ontwerpen van je onderzoek ook rekening met de programma's en applicaties die je gebruikt voor het verzamelen, opslaan en analyseren van je data. Niet alle software-leveranciers gaan netjes om met de data. Gebruik bij voorkeur software die door Fontys goedgekeurd wordt. Niet zeker? Neem dan contact op met hremenpAVG@fontys.nl of hremenpfunctioneelbeheer@fontys.nl.





Stap 3: Toestemming

Maak altijd gebruik van een schriftelijke toestemmingsverklaring. Een template hiervan is in dit document te vinden en tevens op te vragen bij de lectoraten van HRM en Psychologie. Leg hierin in ieder geval het volgende vast:

1. Wat het doel van het onderzoek is (kan ook een overkoepelend onderzoek zijn, waar dit een deelonderzoek van is),
2. Welke partijen toegang hebben tot de data,
3. Welke gegevens worden verzameld,
4. Hoe lang de verzamelde gegevens worden bewaard.

Het is belangrijk dat de respondent snapt waar hij toestemming voor geeft, maar maak het niet zo specifiek dat je bijna niets meer met de data kunt doen. Sla deze toestemming beveiligd op (dus met een wachtwoord of op een andere manier dat niemand er zomaar bij kan)!

Stap 4: Hergebruik

Wil je de data later kunnen hergebruiken? Neem dit dan expliciet op in de toestemmingsverklaring óf vraag opnieuw om toestemming. Verzamelde persoonsgegevens mogen alleen gebruikt worden voor het doel waar de respondenten toestemming voor hebben gegeven. Wil je de data voor een ander onderzoek hergebruiken? Dan moet je ofwel in je originele toestemmingsverklaring dit al opgenomen hebben, ofwel de respondenten opnieuw om toestemming vragen





Stap 5: Veilige opslag

Persoonsgegevens en gecodeerde/gepseudonimiseerde data sla je altijd veilig op. De sleutel van gecodeerde/gepseudonimiseerde gegevens sla je altijd apart op, nooit in hetzelfde bestand als de gecodeerde dataset. Bescherm deze sleutel goed door deze beveiligd op te slaan, met bijvoorbeeld een wachtwoord.

Veilige opslag bereik je ook door de volgende tips:

1. Maak gebruik van door Fontys beschikbaar gestelde programma's, laptops en diensten.
2. Het gebruik van two factor authentication is sterk aan te raden.
3. Maak vooral geen gebruik van gratis diensten, dus diensten waar je niet voor moet betalen om ze te gebruiken, zoals Google Forms. Bedrijven moeten geld verdienen om te kunnen bestaan; als jij het bedrijf niet betaalt voor gebruik van hun product, dan ben jij zelf het product waarmee het bedrijf geld verdient (bijvoorbeeld door je gegevens door te verkopen aan advertentie-bedrijven).
4. Zorg dat alleen bevoegden toegang tot de data hebben. Andere onderzoekers binnen hetzelfde (overkoepelende) onderzoek én binnen de organisaties die aan het onderzoek meewerken hebben recht op toegang tot de data, mits zij de data voor de doeleinden gebruiken waarvoor de respondent toestemming gegeven heeft. Een docent of ondersteuner die op geen enkele manier aan het lectoraat verbonden is, mag niet zomaar onderzoeksdata van het lectoraat inzien, ook al werken ze beiden bij Fontys.

Stap 6: Verwijderen

Verwijder data wanneer je deze niet meer gebruikt of nodig hebt. We leggen een vaste bewaarperiode vast van 7 jaar. Na deze periode moet je de data verwijderen. Houdt daarbij rekening met verplichte bewaartermijnen en met bijvoorbeeld de gedragscode wetenschappelijke integriteit.

Maak het jezelf makkelijk en reserveer één keer per jaar een schoonmaakdag, waarop je alle bestanden die verjaard zijn, verwijderd. Natuurlijk doe je dat niet alleen digitaal, maar ook met alle papieren versies van documenten die je hebt. Om je daarbij te helpen, is het handig om op alle documenten een datum ter verwijdering te noteren. Doe dat bijvoorbeeld in de naam van een document, of schrijf het ergens op je fysieke document.





Stap 7: Recht op vergetelheid

Respondenten hebben het recht om 'vergeten te worden'. In het geval van onderzoek (waarbij je op basis van toestemming gegevens verwerkt), betekent dit dat respondenten het recht hebben om hun toestemming in te trekken.

Indien je redelijkerwijs de gegevens van de respondent uit je dataset kunt verwijderen, dan moet je dit doen. Heb je bijvoorbeeld interviews of vragenlijsten afgenomen en de data wel opgeslagen en eventueel al los van elkaar geanalyseerd, dan kun je de losse data van deze persoon nog herkennen en gemakkelijk uit je dataset verwijderen.

Is de data al zo verweven in het onderzoek en bijvoorbeeld al gepubliceerd, dat het erg lastig of zelfs onmogelijk is om data nog terug te herleiden naar die respondent? Dan is het verwijderverzoek niet meer redelijk uit te voeren en hoef je hier niet aan te voldoen.

Krijg je te maken met een respondent die zijn toestemming intrekt? Neem dan altijd contact op met functioneel beheer. Zij zullen dit verzoek oppakken.

Stap 8: Recht op inzage gegevens

Respondenten hebben het recht om hun gegevens in te zien. Geeft iemand aan dat hij of zij wil inzien welke gegevens er van hem of haar opgeslagen zijn? Verwijs deze persoon dan altijd door naar functioneel beheer, zij pakken dit verder op. Dat doen ze door deze persoon door te sturen naar de Privacy Officer, waar deze persoon begeleid wordt in dit verzoek. De Privacy Officers hebben namelijk registers, waarin staat wat er vastgelegd wordt, van studenten, werknemers en 'overigen' (samenwerkingspartners bijvoorbeeld).





Stap 9: Datalek = melden

Meld een datalek meteen! Als er sprake van een datalek, bijvoorbeeld omdat een (onbeveiligde) USB-stick of een stapel papieren met daarin persoonsgevoelige gegevens in de trein zijn blijven liggen, of omdat je via de mail privacygevoelige informatie hebt verstuurd naar een verkeerde ontvanger? Meldt dit dan meteen!

Voor ons instituut kun je dit melden bij functioneel beheer, via hrmenffunctioneelbeheer@fontys.nl. Doe dit zo snel mogelijk nadat je het datalek hebt ontdekt, maar niet later dan 24 uur na de ontdekking van het datalek.

Zo hebben we intern tijd genoeg om het lek te onderzoeken en, indien nodig, hier een melding van te maken bij de Autoriteit Persoonsgegevens.

Vind je het spannend om te melden? Begrijpelijk, maar een datalek melden is niet erg, sterker nog: het is juist goed. Zo kunnen we het datalek snel verhelpen en met elkaar leren van de situatie. Niet melden is daarentegen wel erg: het niet melden van datalekken kan resulteren in boetes. Gewoon melden dus!



Praktische tips

In dit hoofdstuk vind je praktische tips om veilig met gegevens om te gaan. Sommigen hebben betrek op onderzoek, maar we geven je ook handvaten voor je dagelijkse bezigheden.

Heb je zelf een goed idee of handigte tip, die hier niet bij staat? Laat het ons dan vooral weten, via hremenpAVG@fontys.nl. Zo maken we met elkaar ons instituut steeds een stukje meer AVG-proof.

Ga zorgvuldig om met de gegevens van een ander.

Stuur je bijvoorbeeld een e-mail naar meerdere personen (waaronder ook niet-Fontys medewerkers), zorg dan dat je de ontvangers allemaal in de BCC zet. Zo deel je niet ongevraagd de gegevens met derden.

Gebruik altijd je Fontys laptop. Deze is encrypted, wat betekent dat als je de laptop per ongeluk in de trein laat liggen, anderen niet in de laptop kunnen (en dus ook niet bij eventuele privacygevoelige data). Natuurlijk wel even bij functioneel beheer melden als dit gebeurt! Je eigen laptop is waarschijnlijk minder goed beschermd. Laat je die liggen in de trein, dan is er sowieso sprake van een datalek.

Loop je even weg bij je laptop? Vergrendel je scherm dan (met 'vlaggetje + L'). Zo kan er, ook in die korte tijd dat je weg bent, niemand bij jouw bestanden.

Heb je persoonsgegevens of andere gevoelige informatie op je scherm open staan? Denk er dan aan dat mensen die achter je staan mee kunnen lezen. Dit is in het bijzonder belangrijk wanneer je gebruik maakt van de overleg ruimtes met glazen wanden. Of als bijvoorbeeld je laptop is aangesloten op een extern scherm!

Je kunt veel bestanden beveiligen met een wachtwoord. Denk bijvoorbeeld aan Word- en Excelbestanden. Maak hier gebruik van! Als je niet goed weet hoe dat moet, kijk dan even op internet voor een handleiding of neem contact op met de IT Servicedesk.

Maak gebruik van de software die Fontys aanbiedt, zoals Onedrive of andere (toekomstige) programma's om data te verzamelen, op te slaan en te delen met bijvoorbeeld collega's. Niet alleen handig, maar ook veilig!

Verstuur geen mails met persoonsgegevens in de tekst. Als het nodig is om persoonsgegevens te delen, doe dat dan bijvoorbeeld via Onedrive of verstuur de persoonsgegevens in een (met wachtwoord beveiligde) bijlage.

Het risico van persoonsgegevens mailen is met name dat mails makkelijk doorgestuurd worden, waardoor gegevens uit een eerdere reactie bij de verkeerde ontvangers terecht kunnen komen: een datalek!

De AVG ziet volwassenen als iedereen vanaf 16 jaar oud. Respondenten mogen dus vanaf hun 16e jaar zelf toestemming geven. Voor kinderen <16 jaar oud dienen de ouders/voogd te tekenen. Het kind hoeft dan niet zelf te tekenen. Ethisch gezien zeggen we overigens dat kinderen tussen 12 – 16 jaar ook moeten tekenen, naast de ouders/voogd.

Ook beeld- en geluidsmateriaal vallen onder persoonsgegevens, wanneer je aan het beeld en/of aan het geluid kan zien, horen en/of terug herleiden welke persoon je ziet en/of hoort. Dat betekent dat je toestemming moet hebben voor het verwerken (inclusief verzamelen en opslaan) van de data, dat je de opnamen dus veilig moet opslaan en dat je de opnamen uiteindelijk ook weer moet verwijderen.

Doe je onderzoek op bijvoorbeeld een school? Vraag dan bij de school na of er eventueel al toestemming is gegeven door ouders voor het meedoen aan onderzoek. Is dat niet zo, dan moet je waarschijnlijk van alle kinderen de ouders om toestemming vragen. Is dat wel zo, dan is het al geregeld. Leg dit dan vast in je onderzoek, zodat duidelijk is dat je weet waar je mee bezig bent.

Heb je bestanden met persoonsgegevens die je na (bijvoorbeeld) 7 jaar moet verwijderen? Leg dan duidelijk vast, bij voorkeur in de naam van het bestand, wanneer het bestand verwijderd moet worden. Bijvoorbeeld 'onderzoeksdata onderzoek ABC, verwijderen in 2026'.

Let op bij het publiceren van scripties in de HBO-kennisbank: studenten mogen hun scriptie daar in zetten, mits er geen persoonsgegevens in de scriptie terug te vinden zijn. Dat gebeurt soms wel doordat ze bijvoorbeeld bijlagen aan de scriptie toevoegen, waarin data of bijvoorbeeld toestemmingsverklaringen opgenomen zijn. Wij dienen hier ook op te letten en onze studenten hierop te wijzen!

Wanneer je onderzoek doet met meerdere personen, gelden de volgende regels: Fontys is één bedrijf, dat betekent dat je verzamelde data binnen Fontys mag delen, mits de data gebruikt blijft worden voor het doel waarvoor de respondenten toestemming hebben gegeven en alleen met mensen die er iets mee van doen hebben.

Werk je met meerdere bedrijven samen in bijvoorbeeld een consortium, leg dan duidelijk vast welke partijen in dit consortium samenwerken. Benoem ook alle partijen in bijvoorbeeld de toestemmingsverklaring, zodat het voor respondenten duidelijk is welke partijen de data in kunnen zien/kunnen verwerken.

Spreek ook af met alle samenwerkende bedrijven wat te doen bij een datalek. Neemt bijvoorbeeld één partij dan het voortouw in het melden, of doet iedere partij dat voor zich? Bespreek dit en leg dit vast.

Bij aanvragen voor bijvoorbeeld subsidies worden door de subsidieverstrekkers vaak veel gegevens gevraagd, die niet altijd nodig zijn voor het beoogde doel. Momenteel is dat nog zo, maar wees hier wel kritisch in. Stel bijvoorbeeld vragen aan de subsidieverstrekker over de gevraagde data. Ook wordt er bij subsidieaanvragen vaak gevraagd naar informatie over Research Data Management (RDM). Er is een standaardtekst beschikbaar over RDM via de portal Research Data Management op de pagina Eisen van subsidiegevers. Op de portal zal altijd de actuele versie beschikbaar zijn. Hier staat verder informatie over RDM, instrumenten, opslagsystemen, ethiek, et cetera.



Veelgestelde vragen

Met wie neem ik contact op in het geval van een datalek of andere vragen over de AVG of persoonsgegevens?

Binnen het instituut Fontys Hogeschool HRM en Psychologie kun je bij een datalek contact opnemen met functioneel beheer, via hrmenpfunctioneelbeheer@fontys.nl. Zij helpen je verder of verwijzen je door naar de relevante partijen. Voor andere vragen over de AVG of persoonsgegevens in het kader van onderzoek, kun je contact opnemen met hrmenpAVG@fontys.nl. Zij kunnen je vragen beantwoorden en denken graag met je mee.

Moet je kinderen in de leeftijd van 12-16 jaar ook zelf laten tekenen?

Volgens de AVG moet voor kinderen tot 16 jaar toestemming gegeven worden door een ouder/voogd. Ethisch gezien zeggen we, kinderen tussen 12 en 16 dienen zelf ook toestemming te geven, naast een oud/voogd. Een andere discussie is bijvoorbeeld of één van de ouders, of beide ouders moeten tekenen. Ethisch gezien dienen beide ouders te tekenen, ongeacht de persoonlijke situatie. Kom je er niet uit? Overleg dan met collega's of docenten, of leg je vraag voor aan de commissie ethiek van onderzoek.

Moet ik altijd schalen gebruiken bij het verzamelen van kwantitatieve data, zoals leeftijd in blokken van 5 jaar (1-5, 6-10, 11-15, 16-20 et cetera)?

Probeer je data zoveel mogelijk te anonimiseren. Het gebruik van schalen in plaats van daadwerkelijke data (bijvoorbeeld leeftijd = 17) kan daarbij helpen. Maar als je bijvoorbeeld met een gemiddelde leeftijd wil gaan werken, of het is voor je onderzoek belangrijk dat je de exacte leeftijd weet, dan mag dat gewoon. Het advies is om bij het ontwerpen van je onderzoek alvast goed na te denken over welke data je nodig hebt voor je onderzoek en in hoeverre je dat kan en moet anonimiseren.

Mag je de toestemming ook mondeling doen?

Mondeling toestemming vragen mag, als je maar een opname (in ieder geval geluid) hebt van de toestemming. In die opname moet dan ook de naam van de persoon opgenomen zijn, zodat je weet wie de toestemming gegeven hebt. Als je dit doet, houdt dan rekening met het opslaan van het geluidsbestand: sla dit veilig op en knip bijvoorbeeld het eerste stuk (waarin de toestemming gegeven wordt) los van het totaalbestand.

Mag je de data ook voor vervolgonderzoek gebruiken?

Of je data voor vervolgonderzoek mag gebruiken, ligt een beetje aan hoe je toestemming hebt gevraagd. Als je heel specifiek voor een deelonderzoek toestemming hebt gekregen, zal je opnieuw toestemming moeten vragen. Als je vervolgonderzoek in het verlengde van het originele onderzoek ligt en de toestemming is 'passend' gevraagd, mag je de data hergebruiken. Om zeker te zijn kun je altijd in je toestemmingsverklaring vragen om toestemming voor hergebruik van data voor vervolgonderzoek. Beschrijf dan wel wat voor vervolgonderzoek dat is, zoals je ook het huidige onderzoek beschrijft.

Wat zijn de alternatieven als bijvoorbeeld Google applicaties niet mogen worden gebruikt? Is er een overzicht van door Fontys goedgekeurde programma's?

De dienst O&O is op het moment van schrijven aan het inventariseren wat alternatieven zijn voor het gebruik van online surveytools. Het advies momenteel is: gebruik geen programma's die gratis zijn en neem de voorwaarden en privacyverklaring door. Staan daar ongeregeldeheden, onduidelijkheden of zaken in waar je het echt niet mee eens bent? Gebruik het programma dan niet. Heb je vragen of twijfels? Neem dan contact op met hrmenpfunctioneelbeheer@fontys.nl.

Hoe stel je 2-factor authentication in met Fontys apparatuur (bijvoorbeeld voor OneDrive)?

2-factor authentication (2FA) is een manier om in te loggen met twee stappen, namelijk met iets wat je weet (bijvoorbeeld gebruikersnaam en wachtwoord) en iets wat je hebt (bijvoorbeeld een telefoon waarnaar een SMS-code verstuurd wordt). Het gebruik van 2FA is een veilige(re) manier om gegevens op te slaan en toegangsbeheer tot de data te regelen. OneDrive heeft bijvoorbeeld een optie om 2FA in te stellen. Fontys is momenteel aan het testen met deze optie. Als je hier interesse in hebt of dit aan wil laten zetten, neem dan contact op met de IT servicedesk van Fontys.

Kijk ook eens bij de instellingen van verschillende softwarepakketten die je nu al gebruikt voor dataopslag of verwerking, om te zien of 2FA een optie is. Als die optie er is, is het sterk aan te raden om deze ook te gebruiken.

Betreft de bewaartermijn de minimale duur dat je materiaal moet bewaren, of de maximale periode dat je mag bewaren?

Volgens de AVG is de bewaartermijn de termijn waarop je materiaal maximaal mag bewaren. In veel gevallen zijn er ook wettelijke bewaartermijnen, dat zijn termijnen waarop je de data minimaal moet bewaren. Stel dat je wettelijk gezien onderzoeksdata (waarin persoonsgegevens zitten) 7 jaar moet bewaren, omdat er gedurende 7 jaar navraag gedaan kan worden om je data in te zien. Je moet dus de data minimaal 7 jaar bewaren. Volgens de AVG heb je geen reden om je data dan langer dan 7 jaar te bewaren, dus de minimale termijn is dan meteen ook de maximale termijn.

Worden de data na 7 jaar automatisch verwijderd?

Data wordt niet automatisch verwijderd, zeker niet in het geval van onderzoeksdata die je zelf als onderzoeker hebt verzameld. Binnen de lectoraten willen we processen in gang zetten, waarbij we jaarlijks data gaan verwijderen waarvan de bewaartermijn dat jaar gepasseerd is. Om dit snel en goed te kunnen doen, is het aan te raden om bij het opslaan van gegevens, ook vast te leggen wanneer de gegevens verwijderd mogen worden. Zeker omdat in die langere termijnen sprake kan zijn van een wisseling in personeel of bevoegdheden.

Een tip is daarom om bij het opslaan van documenten (waarin persoonsgegevens staan), in de titel van het bestand meteen een verwijderdatum op te nemen. Het is dan eenvoudig en snel te zien door iedereen die bij het bestand kan, wanneer het verwijderd dient te worden.

Wie is de eigenaar van en wie is eindverantwoordelijk voor de data die door de studenten wordt verzameld?

Juridisch gezien is niemand eigenaar van de data op zich, alleen van de data drager (bijvoorbeeld de computer waar de data opgeslagen staat), maar je kunt wel verantwoordelijk zijn voor de verwerking van data. We gaan afspreken met studenten (en dit ook vastleggen in de praktijkovereenkomst) dat studenten in opdracht van het lectoraat onderzoek doen en dat de verzamelde data daardoor onder de verantwoordelijkheid van het lectoraat/Fontys valt. Dat betekent dat de data door Fontys verwerkt wordt. Wanneer de student afstudeert, levert hij alle data die hij heeft, in. Hij dient dan een verklaring te ondertekenen waarin staat dat hij inderdaad geen data meer heeft. Op deze manier kan Fontys zorgdragen voor het veilig opslaan en tijdig verwijderen van de data.

Moet je voor een breed uitgezette online enquête ook een toestemmingsverklaring hebben?

Indien je met deze online enquête persoonsgegevens verzamelt, dus gegevens die tot een persoon herleidbaar zijn, dan moet je inderdaad toestemming vragen (en krijgen). Als je alle vragen zodanig stelt dat de data anoniem wordt, maar ook echt anoniem, dan geldt de AVG niet en dan heb je ook geen toestemmingsverklaring nodig. Als je het niet zeker weet, neem dan contact op met hrmenpAVG@fontys.nl.

MASONIC
I-K

MASONIC
L

MASONIC
M-Ma

MASONIC
R

MASONIC
S-Sh

MASONIC
Si-Sy

GENERAL
Ar - Bar

Bas - Bo

GENERAL
Bor - Bur

GENERAL
Do - En

GENERAL
Es - Fo

GENERAL
Fr - Go

GENERAL
J

GENERAL
K

GENERAL
L - Len

GENERAL
Mi - Mur

GENERAL
N - Ol

GENERAL
Or - Per

GENERAL
S - So

GENERAL
Sh - So

Sn-Sz

Afbeeldingen

Afbeelding	Auteur	Pagina
Sleutel	Matt Artz, via unsplash.com achtergrondaanpassingen door Mariëlle Rosendaal	1
Roze lamp	Nathan Dumlao, via unsplash.com	6
Sloten zonsondergang	Greg Rosenke, via unsplash.com	8
Iconen stappenplan	Freepik, via flaticon.com	14, 17, 18, 21, 22, 25, 26, 29, 30
Lamp zonsondergang	Diego PH, via unsplash.com	32
Lamp spiraal	Timothy Chan, via unsplash.com	8
Ladekast	Erol Ahmed, via unsplash.com kleuraanpassingen door Mariëlle Rosendaal	44

