Informatie over de Algemene Verordening Gegevensbescherming (AVG)

AVS november 2017, Jan Stuijver

In de Wet bescherming persoonsgegevens (Wbp) zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd. Per 25 mei 2018 wordt de Wet bescherming Persoonsgegevens (WBP) vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG) die in heel Europa van toepassing wordt. Deze nieuwe wetgeving stelt hogere en aanvullende eisen aan privacy.

De AVG stelt tal van uiteenlopende eisen aan organisaties die persoonsgegevens verzamelen of verwerken, inclusief de eis om aan de volgende zes basisbeginselen te voldoen:

Transparantie, behoorlijkheid en rechtmatigheid bij de omgang met en het gebruik van persoonsgegevens. Je moet personen duidelijkheid bieden over de manier waarop je persoonsgegevens gebruikt en je hebt ook een 'rechtmatige basis' nodig om die gegevens te verwerken.

De verwerking van persoonsgegevens moet beperkt blijven tot welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het is niet toegestaan om persoonsgegevens te hergebruiken of openbaar te maken voor doeleinden die niet 'verenigbaar' zijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld.

Minimaliseren van de verzameling en opslag van persoonsgegevens tot wat toereikend en ter zake dienend is gezien de beoogde doelstelling.

Waarborgen van de juistheid van persoonsgegevens met de mogelijkheid om deze te wissen of te rectificeren. Je dient maatregelen te nemen om te waarborgen dat de persoonsgegevens die je bewaart, juist zijn en dat deze bij fouten gecorrigeerd kunnen worden.

Beperken van de opslag van persoonsgegevens. Je dient te waarborgen dat je persoonsgegevens uitsluitend bewaart gedurende de periode die nodig is om de doeleinden waarvoor de gegevens zijn verzameld, te realiseren.

Waarborgen van de veiligheid, integriteit en vertrouwelijkheid van persoonsgegevens. Jouw organisatie moet er door middel van technische en organisatorische veiligheidsmaatregelen voor zorgen dat persoonsgegevens beveiligd zijn.

Artikel 4 van de AVG bevat een lijst met definities van de begrippen en termen zoals die in de verordening worden gebruikt. De volgende begrippen zijn daarbij met name van belang:

'Verwerkingsverantwoordelijke': een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

'Verwerker': een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

'Persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

'Verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, 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.

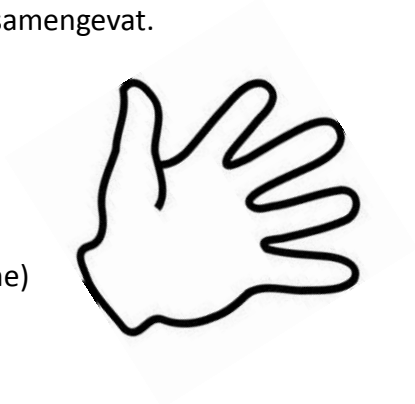
'Pseudonimisering': het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

'Rechtsgrond': Op basis van de AVG mag je geen persoonsgegevens verwerken met als enige reden dat je dat graag wilt. Je moet concreet kunnen aantonen dat je een 'rechtsgrond' voor die verwerking heeft. De AVG voorziet in een aantal redenen wanneer dat verwerken is toegestaan, bijvoorbeeld wanneer de verwerking noodzakelijk is om een contract uit te voeren, wanneer personen toestemming hebben gegeven voor de

verwerking van hun gegevens of wanneer die verwerking in het 'gerechtvaardigde belang' is van de organisatie (mits dat belang niet ten koste gaat van de rechten van de betreffende personen).

In **de 5 vuistregels** worden de belangrijkste (nieuwe) uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat.

1. Doelbepaling en doelbinding;
2. Grondslag
3. Dataminimalisatie
4. Transparantie (recht betrokkene)
5. Data-integriteit.



Doelbepaling en doelbinding:

Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld en concreet doel. Deze persoonsgegevens mogen alleen worden verwerkt om dat vastgestelde doel te bereiken (doelbinding).

Let op: als een school gegevens verzamelt, die niet vallen onder het vrijstellingsbesluit, dan eist de Wbp van de school deze gegevensverzameling apart wordt aangemeld bij het Autoriteit Persoonsgegevens (AP) In de praktijk zal dit niet vaak voorkomen.

Met ingang van 25 mei 2018 is de Wbp niet meer van toepassing en gelden de regels vanuit de Algemene Verordening Gegevensbescherming (AVG). Scholen hoeven dan **geen melding** meer te doen, maar ze zijn verplicht zelf bij te houden welke gegevens waarvoor gebruikt worden: scholen moeten op hoofdlijnen weten welke gegevens voor welk doel worden gebruikt.

Grondslag:

Is er minimaal een wettelijke grond voor de verwerking?

Verwerking van persoonsgegevens is gebaseerd op een van de volgende wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.

Dataminimalisatie:

De persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel (‘proportioneel’) en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt (‘subsidiair’).
Het gaat er dus om dat scholen uitsluitend gegevens verzamelen die écht nodig zijn om het doel te bereiken. Niet: zo min mogelijk gegevens, wel: alleen relevante gegevens.
Dataminimalisatie heeft ook te maken met bewaartermijnen en nog meer met het vernietigen van data als de bewaartermijn is verstreken.

Transparantie:

De betrokkene (dus: de leerling en/of zijn ouders) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. De leerling en zijn ouders zijn op de hoogte van hun rechten als het gaat om de verwerking van persoonsgegevens door de school.

Data-integriteit:

De school zorgt er voor dat bij verwerkingen, die door of namens de school of schoolbestuur worden uitgevoerd, de juiste persoonsgegevens op het juiste moment op de juiste plaats beschikbaar zijn. Onjuiste gegevens worden op tijd gerectificeerd of gewist.
Voorbeeld: als iemand van buitenaf zomaar de persoonsgegevens kan wijzigen, dan zijn die gegevens niet meer 'integer'. De kwaliteit van de gegevens wordt allereerst bepaald door de medewerkers die gegevens invoeren. Zij moeten de juiste instructies krijgen om verantwoordelijk met persoonsgegevens om te kunnen gaan. Ook de programma's die gebruikt worden om de gegevens in op te slaan moeten integer zijn. Door het nemen van passende technische of organisatorische maatregelen zorgt de school er voor dat persoonsgegevens op een passende wijze zijn beveiligd en zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Waar komt het AVG in het kort op neer?

1. U moet exact weten welke bestanden met persoonsgegevens u beheert en in bezit heeft.

2. U moet weten welke rechten de personen hebben van wie u gegevens in bezit heeft.

3. Wanneer u een product of dienst ontwikkelt, dan moet er 'security by design' worden toegepast, oftewel: u moet gelijk nadenken hoe u de beveiliging van gegevens waarborgt en inbouwt.

4. Projecten met hoge risico's op lekken moeten vooraf een inschatting van privacy risico's krijgen, een zogenaamde Privacy Impact Analyse (PIA).

5. U mag persoonsgegevens alleen maar gebruiken voor het doel waar de informatie oorspronkelijk voor verzameld is.

6. Wie persoonsgegevens behandelt, is verplicht aan de strengere regelgeving te voldoen die de Algemene Verordening Gegevensbescherming (AVG) voorschrijft.

7. Artikel 4 van de AVG beschrijft twee rollen, die van de controller en van de processor. Wanneer uw bedrijf persoonsgegevens opvraagt of verwerkt, wordt u gezien als de controller, ongeacht of u zelf direct data verzamelt.

8. U bent als controller volgens de AVG verantwoordelijk voor:

1. Het verzamelen van de gegevens en het toestemming hebben/verkrijgen van de persoon van wie de gegevens zijn.
2. Het zorgen dat deze gegevens alleen voor het doel worden verwerkt waarvoor ze zijn verkregen, en dat ze adequaat worden beveiligd.
3. Het verwijderen van data op verzoek van de persoon van wie de data is.
4. Het aangeven welk niveau van beveiliging vereist is.

Waar te beginnen

De volgende vier belangrijke stappen zijn van belang om te komen tot AVG proof zijn:

1.Traceren – het in kaart brengen van alle persoonsgegevens binnen jouw organisatie met de locaties waar ze zich bevinden.

Welke typen persoonsgegevens worden er binnen onze organisatie verwerkt?

Wat is het doel hiervan?

2.Beheren – het managen van de wijze waarop persoonsgegevens worden gebruikt en van de manier waarop ze toegankelijk zijn.

Van welke betrokkenen verwerken wij eigenlijk persoonsgegevens? Om wie gaat het eigenlijk?
Waar moet u zeker op letten bij de bescherming van persoonsgegevens binnen uw

organisatie per 25 mei 2018.

3.Beveiligen – het nemen van veiligheidsmaatregelen om kwetsbaarheden en gegevensinbreuken te voorkomen, te traceren en aan te pakken.

4.Rapporteren – reageren op verzoeken omtrent gegevens, rapporteren van gegevensinbreuken en beschikbaarheid van de vereiste documentatie
Het eenvoudigst is om te beginnen met een inventarisatie van de gegevens die u nu binnen uw bedrijf heeft. U moet een antwoord te formuleren op de volgende vragen:

Welke valkuilen zijn er?
1: Er valt binnen de AVG meer onder persoonsgegevens dan u misschien denkt. Onder persoonsgegevens vallen niet alleen gegevens die iemand direct identificeren, maar ook gegevens die gebruikt worden om mensen te individualiseren binnen een groep.

Het is dus van belang dat u zicht heeft op alle gegevens die verzameld worden en dat u goed weet welke gegevens allemaal onder persoonsgegevens vallen.

2: Een privacy-statement dat alleen u/de organisatie begrijpt.
Het is inmiddels gebruikelijk om in een privacy-statement aan te geven wat u als bedrijf doet met persoonsgegevens. De AVG schrijft voor dat 'Informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk moeten zijn. Er moet duidelijke en eenvoudige taal worden gebruikt.' Als u eens kritisch naar uw eigen privacy-statement kijkt, hoe begrijpelijk is die tekst dan?

3: Enkel registreren van datalekken met nadelige gevolgen.
De huidige Wet bescherming persoonsgegevens verplicht bedrijven om een administratie bij te houden van iedere inbreuk die leidt tot een aanzienlijke kans op, dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

De AVG breidt de eisen aan deze administratie uit. Per 25 mei 2018 bent u verplicht om alle inbreuken in verband met persoonsgegevens te documenteren en binnen 72 uur te

melden aan de Autoriteit Persoonsgegevens. In deze administratie moeten per geval de feiten, de gevolgen en de maatregelen vastgelegd worden. Opmerkelijk is dat er sprake is van 'alle inbreuken', dus ook de inbreuken waarvoor geen meldingsplicht geldt.

Onder de AVG bent u dus verplicht een veel omvangrijkere administratie bij te houden dan nu het geval is. Ieder incident waarbij iemand "per ongeluk" toegang krijgt tot gegevens moet u strikt genomen registreren. Voor het onderwijs is wellicht een Functionaris Gegevensbescherming dan ook noodzakelijk.

4: Onvoldoende afspraken met uw IT-bedrijf.
De AVG bepaalt dat er afspraken gemaakt moeten worden over de melding van datalekken. Er staat niets vermeld over de inhoud van deze afspraken of de verantwoordelijkheden. Het is daarom verstandig om duidelijke afspraken met uw IT-bedrijf te maken over de informatie die nodig is om een goede en volledige administratie bij te houden. Op welke manier waarborgt uw IT-bedrijf dat de informatie die u nodig hebt bij een eventuele melding beschikbaar is? Verantwoordelijken kunnen anders met lege handen staan als de toezichthouder aanklopt en inzage vraagt in de (wettelijk verplichte) administratie. Ook belangrijk: kan uw IT-bedrijf aantonen dat u alles hebt gedaan om een lek te voorkomen? Dit laatste punt kan uw kans op een eventuele boete bij een inbreuk verkleinen.

Als alles op orde is wat dan?
De regels binnen de AVG staan genoteerd, u weet wat u moet doen om de persoonsgegevens binnen uw organisatie te beschermen, de valkuilen zijn bekend en een actieplan - inclusief een verdeling van verantwoordelijkheden - ligt klaar als er dan toch een datalek ontstaat. U bent al goed op weg als u deze voorbereidingen heeft getroffen. Maar hoe staat u op tijd paraat? Hoe signaleert en herkent u een datalek, zodat u op tijd een melding kunt maken?

Ten eerste is het belangrijk om in beeld te hebben welke persoonsgegevens u allemaal opslaat. Welke kroonjuwelen heeft u onder uw hoede, wie heeft er toegang tot die gegevens en hoelang blijven deze bewaard? Samen met collega's zijn er van tevoren verschillende scenario's te bedenken waar het mis kan gaan.

Schakel daarom ook met uw IT-partners, zij weten precies welke aanvallen van buitenaf mogelijk zijn, kunnen systemen voor u monitoren en weten vanuit hun ervaring met andere klanten ook waar de pijnpunten binnen een organisatie zitten. Zodra u hier een goed overzicht van hebt, weet u precies waar een datalek kan ontstaan en dus ook waar u alert op moet zijn.

Bij organisaties van een redelijk formaat is het echter onvoldoende om alleen alert te zijn. Nóg belangrijker is het dat álle medewerkers die met persoonsgegevens omgaan bewust zijn van de privacygevoeligheid, dat zij volledig geïnformeerd zijn over de nieuwe regelgeving en hier samen met u alert op zijn. Ook is het belangrijk dat u een cultuur creëert waarbij medewerkers zich veilig voelen om een datalek te melden. Het is bekend dat menselijke fouten of slordigheden het merendeel van de datalekken veroorzaken. Uw IT-processen kunnen dan wel spic en span zijn, maar vergeet niet dat een verkeerd geadresseerd mailtje of het achterlaten van een usb stick ook zorgen voor een datalek.

Datalek voorkomen. Wat is dan van belang?

- Het opstellen van strakke richtlijnen binnen een organisatie is een belangrijke eerste stap. Bewustwording speelt hierin een centrale rol; zorg ervoor dat medewerkers zich bewust zijn van hun gedrag wanneer ze omgaan met persoonsgegevens. Een niet-versleutelde PC kan onbewust een kwaadwillend persoon toegang verschaffen tot persoonsgegevens. Medewerkers die in de fout gaan moeten ook weten bij wie ze zich kunnen melden. Hoe langer zij wachten met melden, hoe groter de gevolgen voor alle betrokken partijen. Eventueel volgt ook nog een boete als het datalek niet binnen 72 uur gemeld is bij de Autoriteit Persoonsgegevens.

  Gelukkig zijn er allerlei hulpmiddelen om de bewustwording van medewerkers te vergroten. In Microsoft Exchange vindt u bijvoorbeeld opties die alarm slaan wanneer mensen per ongeluk documenten met woorden als 'vertrouwelijk' of 'intern' versturen. Moderne firewalls hebben 'data leakage prevention', wat het lekken van data tegen gaat. Het is ook aan te raden uw netwerk te (laten) monitoren op afwijkend gedrag. U krijgt dan direct een seintje wanneer er bijvoorbeeld sprake is van een enorme toename van dataverkeer van binnen naar buiten. Verder zijn er diverse (goedkope) tools - waaronder de Canary - die waarschuwen wanneer er een hacker in uw netwerk zit.

- Denk niet alleen digitaal

  Tegenwoordig gebeurt bijna alles online. Ook persoonsgegevens worden inmiddels bijna alleen nog maar online verwerkt. Toch zijn er ook zat voorbeelden van papieren datalekken. Denk bijvoorbeeld aan een verkeerd bezorgde brief met gevoelige patiëntinformatie of een map met persoonsgegevens die uit een auto gestolen wordt. Ook hier gaat het om datalekken.

- Maak goede afspraken met het personeel.
- Zorg dus voor duidelijke afspraken met andere partijen.

  Misschien maakt u gebruik van externe partijen die namens u persoonsgegevens verwerken. Die partijen moeten passende beveiligingsmaatregelen treffen en u in het

geval van een datalek tijdig informeren. Zorg dus voor duidelijke afspraken met deze partijen, en dat zij bijvoorbeeld weten aan wie zij een eventueel datalek moeten melden.

Waar rekening mee houden?
De AVG voorziet in een aantal belangrijke aspecten die niet vergeten mogen worden:

1. Alle betrokkenen hebben uitgebreide rechten:

a. Zij mogen gegevens corrigeren als de verzamelde persoonsgegevens onjuist blijken te zijn (artikel 16).

b. Zij hebben ook het recht om 'vergeten te worden'; op verzoek dient u gegevens zo spoedig mogelijk ('zonder onredelijke vertraging') te wissen (artikel 17).

c. Zij hebben ook het recht om de eigen gegevens in een gestandaardiseerd formaat te ontvangen. Dan is het eenvoudiger om gegevens door te geven aan een andere leverancier van een vergelijkbare dienst, bijvoorbeeld wanneer zij overstappen (artikel 20).

d. En uiteraard hebben zij het recht om de eigen gegevens in te zien (artikel 15). U heeft ook een Registerplicht (artikel 30). Dat betekent dat u schriftelijk de belangrijkste aspecten van de persoonsgegevens die u verwerkt, moet vastleggen. Dit geldt niet voor organisaties met minder dan 250 medewerkers, tenzij:

a. U stelselmatig en op grote schaal (bijzondere) persoonsgegevens verwerkt.

b. De gegevensverwerking een groot risico voor de betrokkenen inhoudt.

Waar nog meer rekening mee houden?
U heeft nog steeds een meldplicht bij datalekken, net als in de huidige Wbp, maar:
1. De drempel wanneer u moet melden is lager geworden. U dient nu elk datalek te melden, mits er geen enkel risico is voor de 'vrijheden en rechten van individuen' (artikel 33).

2. Het datalek moet gemeld worden 'zonder onnodige vertraging' en binnen 72 uur nadat u deze heeft geconstateerd.

3. Bij een hoog risico voor de rechten en vrijheden van individuen moet u ook alle betrokkenen op de hoogte stellen (art. 34). Wat 'hoog' is dient u zelf in te schatten.

4. Wanneer u overheidsinstantie bent of een bedrijf dat het observeren van personen als (kern)activiteit heeft, dan moet u een Functionaris Gegevensbescherming (FG) aanstellen. Dit geldt ook wanneer u grote hoeveelheden gegevens verzamelt.

Incidenten en datalekken.
Een **beveiligingsincident** is een gebeurtenis waarbij de mogelijkheid bestaat dat de

beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.

Een **datalek** is een beveiligingsincident, waarbij gegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden enz.).
Let op: Alle datalekken zijn beveiligingsincidenten, maar niet ieder beveiligingsincident is een datalek.

Een school is verplicht binnen 72 uur een datalek te melden bij de Autoriteit Persoonsgegevens

Tip
Maak een centraal meldpunt met een standaard proces om datalekken **en** incidenten te melden en om vragen te stellen.

- ✓ Spreek af waar informatie en afspraken over AVG te vinden zijn:
  Bijvoorbeeld: incidenten@schoolX.nl
  - Eén adres om te communiceren
  - Eén proces voor de duidelijkheid
  - Eén register voor het overzicht
- ✓ De Functionaris voor de Gegevensbescherming ziet zo alles voorbij komen en kan als een 'spin in het web' bijsturen waar nodig.

Van belang om te weten over publicatie beeldmateriaal.
De Autoriteit Persoonsgegevens wijst in haar berichtgeving op het feit dat het voor scholen en ouders vaak onduidelijk is wat wel en niet mag bij publicatie van beeldmateriaal van leerlingen. De Autoriteit wijst op twee regels:

1. Scholen moeten expliciete toestemming hebben voor het publiceren van foto's of video's van leerlingen. Aandachtspunten hierbij:
a. Het gaat om toestemming van elke leerling die herkenbaar op de foto staat.
b. De toestemming moet ondubbelzinnig zijn. "Dat betekent dat een school niet uit mag gaan van het principe 'wie zwijgt, stemt toe'.
c. Duidelijk moet zijn voor welke specifieke verwerking en doel de toestemming geldt. Toestemming voor het publiceren van foto's van een schoolreisje binnen een afgeschermde omgeving is dus nog geen toestemming voor publicatie van één van die foto's op de schoolsite.

2. Scholen moeten passende technische en organisatorische maatregelen treffen om beeldmateriaal van leerlingen, dat zij verzamelen en gebruiken, te beschermen.

De rol van de medezeggenschap

Alle huidige privacyreglementen voor het verwerken van de personeels-en leerlinggegevens moeten worden aangepast aan de AVG. Dit houdt in dat besturen gewijzigde concepten aan de (G)MR voor moeten leggen. De personeelsgeleding heeft een instemmingsbevoegheid waar het gaat om het wijzigen van een regeling over het verwerken van en de bescherming van persoonsgegevens van het personeel (art. 12 lid 1 onder m WMS).De oudergeleding van de (G)MR heeft in het primair onderwijs een instemmingsbevoegheid met betrekking tot het wijzigen van ene regeling over het verwerken en de bescherming van persoonsgegevens van ouders en leerlingen (art. 13 lid 1 onder i Wms). In het voortgezet onderwijs komt die bevoegdheid toe aan de leerlinggeleding (art. 14 lid 3 onder de Wms).

Zie wet: Verordening (EU) 2016/679 algemene verordening gegevens bescherming
https://www.pmpartners.nl/definitieve-tekst-algemene-verordening-gegevensbescherm

Voor praktische hulpmiddelen en tips zie kennisnet:
https://www.kennisnet.nl/organiseren-ict/informatiebeveiliging-privacy-ibp/