Nederlandse Vereniging
van Arbeidsdeskundigen

STICHTING
REGISTER
ARBEIDSDESKUNDIGEN

Algemene Verordening Gegevensbescherming

Inleiding

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens – Wbp- geldt dan niet meer.

Doel

Het doel van de AVG is om personen te beschermen en duidelijke richtlijnen te scheppen voor organisaties die persoonlijke gegevens verwerken. De AVG waarborgt dat persoonlijke gegevens zorgvuldig worden verwerkt, niet worden misbruikt en niet langer bewaard worden dan nodig is. De AVG betekent dan ook een flinke verzwaring van de regels waaraan organisaties moeten voldoen in het kader van de bescherming van persoonsgegevens.

Wat betekent de AVG voor de arbeidsdeskundige?

Met de AVG in aantocht moet er de komende tijd een groot aantal zaken geregeld worden, zodat de arbeidsdeskundige of de organisatie waarin de arbeidsdeskundige werkzaam is AVG proof is.

De nieuwe wet verwacht van organisaties dat zij actief de nodige stappen ondernemen en alles omtrent privacy uitzoeken, organiseren en vastleggen. Het is een inspanningswet. Het is dus belangrijk aantoonbaar te maken dat u er alles aan gedaan hebt om een overtreding van de wet te voorkomen. Als u zich er niet aanhoudt kunnen er aanzienlijke boetes opgelegd worden (tot het maximale boetebedrag van 20 miljoen euro of 4 procent van de wereldwijde omzet).

Arbeidsdeskundigen hebben de volgende vragen. NVvA en SRA hebben de antwoorden uitgezocht via internet en laten toetsen door mr. dr. Erik-Jan Wervelman. Het onderwerp komt onder zijn leiding ook aan de orde in platform AD 11 op 28 maart 2018 en tijdens een workshop op het Johannes van der Wal Congres op 5 juni 2018.

Vraag 1. In hoeverre richt de AVG zich op organisaties of ook op zelfstandigen? En in dit laatste geval: welke bepalingen zijn dan van toepassing?

De AVG richt zich op organisaties, maar definieert dit begrip niet. Met “organisatie” wordt niet alleen een publieke organisatie bedoeld, maar ook een particuliere organisatie, oftewel – kort gezegd – een “onderneming” . Het begrip “onderneming” omschrijft de AVG in art. 4 onder 19 als: een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen. Een zelfstandige arbeidsdeskundige drijft aldus een onderneming in de zin van de AVG en is dus gebonden aan de regels die gelden voor organisaties met minder dan 250 medewerkers.

Vraag 2. Hoe moet ik, ten behoeve van de AVG vastleggen hoe ik gegevens verwerk?

Organisaties met meer dan 250 medewerkers. Heeft uw organisatie meer dan 250 medewerkers? Dan bent u verplicht om een verwerkingsregister bij te houden.

Organisaties met minder dan 250 medewerkers
Heeft uw organisatie minder dan 250 medewerkers? Dan moet u over een verwerkingsregister beschikken wanneer u persoonsgegevens verwerkt:

- die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;
- waarvan de verwerking niet incidenteel is en/of;
- die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Bent u verplicht om een verwerkingsregister op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.

Wat zijn persoonsgegevens?

Dit zijn zowel de gegevens die in de wet zijn aangemerkt als persoonsgegevens als gegevens die via de context zijn terug te voeren naar een natuurlijk levend persoon. Onder persoonsgegevens vallen onder andere naam, adres, woonplaats, telefoonnummer en geboortedatum

Lees verder: (Sivi green paper: https://www.sivi.org/media/publicaties/sivi%20greenpaper%20ropg%201%20mei%202017.pdf)

Wat zijn bijzondere persoonsgegevens?

Bron: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens.

Bijzondere persoonsgegevens zijn gegevens over iemands:

- godsdienst of levensovertuiging;
- ras;
- politieke voorkeur;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakbond;
- strafrechtelijk verleden.
- Ook het burgerservicenummer (BSN) is een bijzonder persoonsgegeven, omdat het een uniek en tot de persoon herleidbaar nummer is.

Een organisatie mag geen bijzondere persoonsgegevens verwerken, tenzij daarvoor in de wet een uitzondering is.

Vraag 3. Wat moet er in het register van verwerkingsactiviteiten staan?

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht#ben-ik-verplicht-om-een-register-van-verwerkingsactiviteiten-op-te-stellen-6101

Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die u verwerkt. U mag zelf weten hoe u het register opstelt. Wel schrijft de AVG voor welke informatie u als verantwoordelijke of verwerker in het register moet zetten. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet u het register direct kunnen laten zien.

Is uw organisatie de 'verwerkingsverantwoordelijke'?

Stelt uw organisatie zelf het doel en de middelen voor de verwerking van de persoonsgegevens vast? Dan is uw organisatie de verwerkingsverantwoordelijke. De wet schrijft voor dat deze verantwoordelijken de volgende informatie in het register moeten opnemen: de naam en contactgegevens van:

- uw organisatie, of de vertegenwoordiger van uw organisatie;
- eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
- de Functionaris voor de gegevensbescherming (FG) als u die heeft aangesteld;
- eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
- de doelen waarvoor u de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten of direct marketing;
- een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten;
- een beschrijving van de categorieën van persoonsgegevens. Zoals NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen;
- de datum waarop u de gegevens moet wissen (als dat/deze bekend is);
- de categorieën van ontvangers aan wie u persoonsgegevens verstrekt;
- deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het register;
- Indien mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen die u hebt/heeft genomen om persoonsgegevens die u verwerkt te beveiligen.

U neemt in het register overigens niet de daadwerkelijke persoonsgegevens op, maar alleen een beschrijving die inzicht geeft in uw verwerkingsactiviteiten.

Vraag 4. Wat zijn datalekken en hoe moet ik die eventueel vastleggen?

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Bij een datalek gaat het *om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens* bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden datalekken

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick met persoonsgegevens, de diefstal van een laptop of aan een inbraak in een databestand door een hacker.

Meldplicht datalekken

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken?qa=Datalek

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Melden datalekken

Organisaties die een datalek willen melden bij de Autoriteit Persoonsgegevens kunnen dat doen via het meldloket datalekken. In het privacystatement formulier meldplicht datalekken is te vinden hoe de Autoriteit Persoonsgegevens omgaat met de persoonsgegevens van degene die een datalek meldt.

Let op: vanaf 25 mei 2018 gaat de nieuwe Europese privacywet in, de Algemene verordening gegevensbescherming (AVG). Hoewel de meldplicht datalekken blijft bestaan, verandert er mogelijk ook wat voor u. Lees meer over de meldplicht datalekken in ons AVG-dossier.

Meldplicht datalekken na 25 mei 2018:
De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan

Vraag 5. Is het raadzaam om aanvullend op mijn algemene voorwaarden een privacy reglement of een privacyverklaring op te stellen?

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg?qa=privacy%20by%20design&scrollto=1

u U dient een Privacy by design en Privacy by default instellen. Dat is nieuw.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.

Bron https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-design

Privacy by design houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht schenkt aan privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ook houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Daardoor kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.

Organisatiebelang
Privacy by design draagt ook bij aan uw organisatiebelang. Onderkent u de privacy risico's van een product of dienst niet in een vroegtijdig stadium, maar pas als de ontwikkeling ervan al een eind gevorderd is? Dan is de kans groot dat noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door: een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is; op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken; als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Vraag 6. Moet ik voor elke opdracht opnieuw een verklaring opstellen?

Nee, zie bij Verwerkersovereenkomst – en register en Privacy by Design en Privacy by Default.

Vraag 7. Zijn er voorschriften voor het inloggen op een eigen server?

Ja, zie bij Verwerkersovereenkomst – en register en Privacy by Design en Privacy by default.

Vraag 8. Externe (ICT, boekhouder) partijen die soms op afstand inloggen of bij je gegevens kunnen, moet daar ook nog wat voor geregeld worden?

Ja, zie bron: https://ictrecht.nl/factsheets/algemene-verordening-gegevensbescherming-verandert-er-echt/

Als u een verwerker inschakelt voor uw gegevensverwerkingen, dan moet u met deze verwerker een verwerkersovereenkomst sluiten. In de verwerkersovereenkomst (heet tot ingang van de AVG nog bewerkersovereenkomst) maakt u specifieke afspraken over de omgang met persoonsgegevens. Een belangrijk aandachtspunt daarbij is dat wanneer u als verwerker diensten uitbesteedt waarbij persoonsgegevens van een klant zijn betrokken, u hiervoor toestemming nodig hebt van die klant.

Vraag 9. Veranderen de bewaartermijnen onder de AVG? Mag/moet ik rapportages bewaren? En zo ja, hoe lang?

Bewaartermijn persoonsgegevens

Bron: **https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg**

Nee. Zodra de Algemene verordening gegevensbescherming (AVG) van toepassing is, gelden dezelfde regels voor het bewaren van persoonsgegevens als nu. Het uitgangspunt blijft dat u persoonsgegevens niet langer mag bewaren dan noodzakelijk voor het doel van uw verwerking.

Bewaartermijnen vastleggen en mensen informeren

Hoe lang u gegevens mag bewaren, verschilt per geval.

Als verantwoordelijke moet u onder de AVG wel het volgende regelen:

- U bepaalt van tevoren hoe lang u de persoonsgegevens bewaart. Als dat niet mogelijk is, bepaalt u in elk geval de criteria voor het vaststellen van de bewaartermijn. U legt de bewaartermijn of de criteria vast in een bewaarbeleid.
- U neemt de bewaartermijnen ook op in uw register van verwerkingen.
- U informeert de betrokkenen (de mensen van wie u gegevens verwerkt) over de bewaartermijnen. Bijvoorbeeld via een privacyverklaring op uw website.

Verder lezen: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens

Is de bewaartermijn van persoonsgegevens voorbij of zijn de gegevens niet meer noodzakelijk? Dan moet u de gegevens vernietigen. Organisaties mogen persoonsgegevens in een archief bewaren als dit bestemd is voor historische, statistische of wetenschappelijke doeleinden. Tenzij de Archiefwet of een andere wet van toepassing is, geldt voor persoonsgegevens in een archief geen bewaartermijn. De organisatie moet de gegevens vernietigen als ze niet meer nodig zijn voor het doel van het archief.

Vraag 10. Email-communicatie: welk inzicht moet ik daarin geven?

Risico's zijn opgenomen in dit interview van Sens: https://dutchitchannel.nl/588142/e-mail-wordt-in-discussies-over-avg-vaak-vergeten.html

Onder de AVG moeten organisaties ook de persoonsgegevens in e-mailsystemen inzichtelijk maken. Op de eerste plaats om ze te kunnen beschermen tegen diefstal of verlies, bijvoorbeeld door het bijhouden van een kopie of het versleutelen van de data. Maar er is volgens Sens nog een dwingende reden. "Zonder dit inzicht is het onmogelijk om volledig inzicht te geven in verwerkingen van persoonsgegevens. Betrokkenen hebben hier op basis van artikel 15 van de AVG wel recht op."

Een organisatie moet binnen een maand gehoor geven aan een inzageverzoek en mag geen onkosten in rekening brengen voor een kopie van de verwerkte persoonsgegevens. Bij dit inzagerecht blijft het echter niet. Zo moet een organisatie persoonsgegevens ook kunnen verwijderen als een betrokkene hierom vraagt.

Vraag 11. Zijn SRA en NVvA voornemens te faciliteren in de vorm van een update van de handleiding omgang persoonsgegevens en eventueel een gedragscode/procedure?

Ja, SRA en NVvA zijn voornemens om dit in een Klein Slim Groepje samen met mr. dr. Erik Jan Wervelman en een andere deskundige uit te werken.

Vraag 12: Als ik zelf meer wil lezen over de AVG, wat kan ik dan het beste doen?

Er is een handleiding te downloaden (met o.a. stroomschema's):

https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming