DePrivacyGuru

AVG
Voor de HR professional

Mr. Nico J. Mookhoek CIPP/E

Inhoudsopgave

Uit de AVG privacy scans die wij met DePrivacyGuru uitvoeren, blijkt dat de focus van organisaties bij de Algemene Verordening Gegevensbescherming (AVG) vooral ligt op de persoonsgegevens van hun klanten.

Maar de Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG) gelden ook voor de gegevens die je van jouw medewerkers vastlegt!

In haar toelichting op de AVG schrijft de Autoriteit Persoonsgegevens (AP) die belast is met het toezicht, dat de AVG geldt voor verwerking van gegevens die niet incidenteel is. De AP merkt daarbij op dat verwerking van gegevens zelden incidenteel zal zijn. En geeft daarbij expliciet het volgende voorbeeld: "Denk bijvoorbeeld aan de persoonsgegevens van medewerkers die u verwerkt".

Kortom, ook HR krijgt volop te maken met de AVG. In deze White paper behandelen we een aantal zaken waar de HR professional mee te maken krijgt.

Eisen aan een personeelsdossier

De Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) stellen de volgende voorwaarden voor een personeelsdossiers.

1. De gegevens in het personeelsdossier moeten juist en nauwkeurig zijn

Deze eis spreekt voor zich het dossier moet correct zijn.

2. Er mogen niet meer gegevens in het personeelsdossier worden vastgelegd dan nodig is, en de gegevens moeten ter zake doen.

In het personeelsdossier mogen alleen gegevens worden opgeslagen die direct verband houden met de arbeidsovereenkomst. Dat zijn zaken als NAW-gegevens, bankrekeningnummer, een Verklaring Omtrent gedrag (VOG) als deze vereist is, maar ook verslaglegging van functionerings- en beoordelingsgesprekken mogen hier in opgenomen worden.

Het opnemen van medische gegevens in het dossier, anders dan een ziek- en herstelmelding, is niet toegestaan.

3. de persoonsgegevens passend beveiligd worden zodat ze niet verloren raken of in verkeerde handen terechtkomen

De AVG zegt hierover dat de beveiligingsmaatregelen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, moeten waarborgen

Daarbij moet rekening worden gehouden met:

- de stand van de techniek

- de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens

Al met al een vrij open norm waar jouw organisatie, rekening houdende met bovenstaande zelf invulling aan kan geven.

4. De persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is.

Het lastige bij deze bepaling is dat voor de verschillende onderdelen van het personeelsdossier, verschillende maximale bewaartermijnen gelden. Hieronder som ik ze op.

1 jaar na beëindiging van het dienstverband

Het betreft documenten die te maken hebben met de sollicitatiegegevens van een werknemer:

- Sollicitatiebrief of sollicitatieformulier
- Curriculum Vitae (CV)
- Referenties
- Correspondentie uit de sollicitatieprocedure
- Getuigschriften
- Verklaring Omtrent het Gedrag (VOG)
- Psychologisch onderzoek
- Assessments

2 jaar na beëindiging van het dienstverband

Deze termijn geldt voor het overgrote deel van de werknemersgegevens in het personeelsdossier. Hieronder vallen:

- De arbeidsovereenkomst (inclusief wijzigingen)
- Correspondentie over benoemingen, promotie/demotie en ontslag
- Afspraken over het lidmaatschap van de ondernemingsraad
- Verslagen van functioneringsgesprekken en beoordelingsgesprekken
- Verslagen in het kader van de Wet verbetering poortwachter
- Correspondentie met de bedrijfsarts en het UWV over ziekteverzuim en re-integratie
- Verslagen over probleemsituaties (inclusief financiële problemen)

Als het dienstverband beëindigd wordt met een conflict dan raad ik je aan het personeelsdossier te bewaren tot het conflict afgerond is.

5 jaar na beëindiging van het dienstverband

De volgende documenten moet je tot vijf jaar na het einde van het dienstverband van een werknemer in het personeelsdossier bewaren:

- Loonbelastingverklaringen (ook als deze zijn vervangen door nieuwe)
- Kopie van het identiteitsbewijs

7 jaar na beëindiging van het dienstverband

De Belastingdienst beschouwt bepaalde onderdelen van de bedrijfsadministratie, waaronder ook het personeelsdossier, als zogeheten 'basisgegevens'. Dit zijn gegevens die van fiscaal belang zijn. Hieronder valt onder meer de salarisadministratie. Deze moet je minimaal zeven jaar bewaren. Dat geldt ook voor de volgende gegevens.

- Persoonlijke gegevens ex-werknemer (stamkaart)
- Datum van indiensttreding
- Salarisadministratie
- Arbeidsvoorwaarden (aanvullende arbeids- en salarisafspraken)
- Afstandsverklaring woon-werkverkeer

Let op: deze bewaartermijnen gelden ook voor organisaties waar jij zaken aan uit besteed zoals bijvoorbeeld de salarisadministratie aan uit besteed hebt. Als verwerkingsverantwoordelijke ben jij er verantwoordelijk voor dat ook deze organisatie de bewaartermijn hanteert. Controleer dat dus!

Sollicitanten

De gegevens van sollicitanten mag je maximaal 4 weken na afloop van de sollicitatieprocedure bewaren. Je mag wel toestemming vragen om de gegevens langer te bewaren.

Je mag sollicitanten niet om een kopie identiteitsbewijs vragen. Twee uitzendbureaus zijn daar onder de voorganger van de AVG, de WbP, voor op de vingers getikt.

Uitgebreidere rechten werknemer

Onder de AVG heeft de medewerker het recht om zijn volledige personeelsdossier in te zien. Dit recht bestond al onder de Wet Bescherming Persoonsgegevens (WbP). Onder de AVG heeft de medewerker ook recht op een kopie van zijn personeelsdossier. Dat hoeft geen papieren kopie te zijn maar mag ook een elektronische kopie zijn, mits deze een gangbaar formaat heeft (bijv. een pdf).

Aan het recht van inzage zijn wel een aantal beperkingen:

1. als het verzoek buitensporig of ongegrond is, bijvoorbeeld omdat de werknemer niet als doel heeft om zijn persoonsgegevens te controleren en eventueel aan te vullen, te wijzigen of te laten verwijderen dan mag dit gemotiveerd afgewezen worden.
2. Interne notities hoeven niet ter inzage gegeven te worden
3. Stukken waardoor de rechten of vrijheden van anderen (inclusief de werkgever zelf) worden beperkt mogen worden weg gestreept; als dat niet mogelijk hoeven ze niet ter inzage worden gegeven

De werkgever moet medewerkers ook de mogelijkheid bieden hun gegevens te rectificeren te beperken of te verwijderen.

Rectificatie kan in de volgende gevallen. Als de persoonsgegevens:

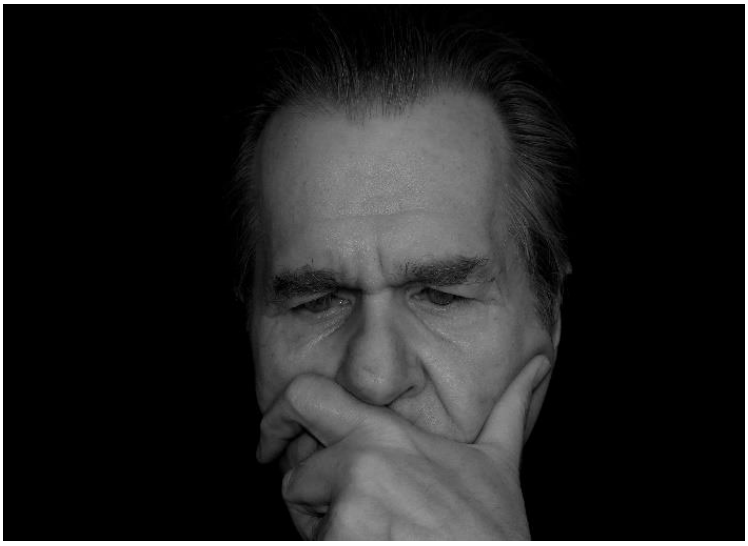
- niet kloppen
- niet compleet zijn
- niet relevant zijn voor het doel waarmee ze verzameld zijn

- in strijd met een wet worden gebruikt

Bovendien moet je de werknemer informeren dat hij een klacht in kan dienen bij de toezichthouder, de Autoriteit Persoonsgegevens.

De werkgever is verplicht binnen één maand te reageren op dergelijke verzoeken van de werknemer. Als je geen gehoor geeft aan een verzoek moet je dit schriftelijk melden en de werknemer meteen attenderen op de mogelijkheden die hij heeft: een klacht indienen bij de AP of een gang naar de rechter.

Rechtsgrond & Informatieplicht



Persoonsgegevens mag je niet zo maar verwerken, je moet een rechtsgrond of zogenaamde grondslag hebben. Dit is de basis waarop je de gegevens mag verwerken. De AVG kent 6 grondslagen.

In de arbeidsverhouding is de grondslag "uitvoering van de overeenkomst". Immers je hebt met de medewerker een arbeidsovereenkomst afgesloten. Op basis daarvan mag je zijn persoonsgegevens, zoals naam, adres, salaris verwerken.

Maar let op: je mag alleen gegevens verwerken die je nodig hebt voor de uitvoering van de arbeidsovereenkomst. Als je bijvoorbeeld een foto van medewerkers wilt plaatsen op de website of in een nieuwsbrief kan dit niet op deze grondslag. Daarvoor moet je de grondslag toestemming gebruiken: je moet toestemming aan de medewerker vragen.

De eisen aan toestemming door de medewerker zijn echter onder de AVG behoorlijk aangescherpt. De toestemming moet volgens de AVG worden gegeven "in vrijheid". Omdat in de relatie werkgever/werknemer een gezagsverhouding is, wordt die vrijheid minder snel verondersteld.

Een algemene formulering voor de toestemming in een arbeidsovereenkomst zal dus niet meer voldoen. Je moet voor elk gebruik dat niet direct gerelateerd is aan de arbeidsovereenkomst, specifieke toestemming aan je medewerker vragen. Die toestemming moet je voor elk soort gebruik vragen. Dus als je in

het bovengenoemde voorbeeld toestemming hebt voor het gebruik van foto's voor de website, maar je wilt die bijvoorbeeld ook gebruiken voor LinkedIn, dan moet je daar apart toestemming voor vragen.

Zorg er ook voor dat je de toestemming vastlegt. De AVG vraagt om aantoonbaarheid.

De toestemming kan te allen tijde ingetrokken worden door de medewerker. Dat betekent dat je vanaf dat moment bijvoorbeeld de foto niet meer mag gebruiken. Het gebruik voor de intrekking van de toestemming mag je gewoon continueren. Je bedrijfsbrochure met de foto hoef je dus niet aan te passen. Pas als je een nieuwe brochure laat maken, mag je de foto niet meer gebruiken.

Daarnaast verwerk je bepaalde persoonsgegevens op basis van een wettelijke verplichting. In de loonadministratie verwerk je de persoonsgegevens op basis van een wettelijke plicht.

Informatieplicht

De AVG eist ook dat je de medewerkers informeert over welke gegevens zij verzamelen, voor welke doeleinden en op basis van welke grondslag etc.

Ik raad daarom altijd aan om naast een privacyverklaring voor de klanten een privacyverklaring voor de medewerkers op te stellen. Je kunt deze verklaring bijvoorbeeld op het Intranet zetten of opnemen in het personeelshandboek.

Op onze website vind je een kant-en-klaar model privacyreglement personeel.

Ontslag wegens privacyschending?

Kun je een medewerker die het privacy beleid van jouw organisatie schendt, ontslaan?

Kantonrechter: ontslag op staande voet houdt geen stand

In twee eerdere uitspraken waar het weliswaar om ontslag op staande voet ging, heeft de kantonrechter het ontslag namelijk ongeldig verklaard.
De eerste uitspraak was in 2015 door de kantonrechter in Amsterdam. Een medewerker van de Sociale Verzekeringsbank (SVB) heeft voor privédoeleinden de gegevens van 23 personen, buren en vrienden, uit het systeem gehaald. De kantonrechter vond dat de medewerker weliswaar het vertrouwen van de werkgever ernstig had geschaad, maar dat het ontslag op staande voet niet in stand kon blijven. Volgens de rechter was, en nu komt het: de SVB tekort geschoten in het trainen van haar medewerkers op het gebied van privacy. "Een werkgever moet haar personeel opvoeden tot privacygevoelige mensen", cursussen en trainingen zijn daarvoor noodzakelijk.

Een pop-up met een standaard waarschuwing elke keer als ingelogd wordt, was niet voldoende volgens de rechter. Sterker nog, die boet in waarde in als er niet daadwerkelijk controles en sancties volgen.

Een paar maanden later in hetzelfde jaar oordeelde de Rechtbank in Noord-Nederland vergelijkbaar. Een medewerkster van een bankinstelling is op staande voet ontslagen omdat ze allerlei gegevens, inclusief een BKR-toetsing van de nieuwe partner van haar ex-man had opgezocht. Ook hier oordeelde de kantonrechter dat het ontslag geen stand kon houden.

Eenmalige regels, richtlijnen en training voldoen niet!

Hoewel de uitspraken van kantonrechters gebaseerd zijn op de feiten van de specifieke situatie, kan uit deze uitspraken afgeleid worden dat privacy bewustzijn onderhouden met worden.
Als dit onvoldoende aangetoond kan worden dan zal een ontslag op staande voet geen standhouden.

Veel organisaties hebben bij de invoering van de AVG hard gewerkt om te voldoen: Registers en privacy verklaringen zijn opgesteld, verwerkersovereenkomsten afgesloten etc. Indien nodig is een Functionaris Gegevensbescherming aangesteld en vaak is voorlichting over de AVG gegeven aan de medewerkers.

En nu..... zijn we meestal weer allemaal over "tot de orde van de dag".

De bovenstaande uitspraken geven weer eens aan dat het toch noodzakelijk is om continu aandacht te blijven vragen voor het privacy bewustzijn van je medewerkers. Het creëren en houden van dat bewustzijn is een continu proces. Dat betekent dat je als privacy verantwoordelijke, als HR of FG een programma moet hebben om de bewustwording te creëren en te onderhouden. Een programma met regelmatige trainingsmomenten, audits op de naleving van maatregelen en rapportage daarover aan het management.

Bewustwording creëren noodzaak

Overheden en bedrijven spenderen kapitalen aan informatiebeveiliging. Legio technische maatregelen worden getroffen, om te voldoen aan de AVG worden documenten en procedures opgesteld. De menselijke factor waarmee de uitvoering staat of valt wordt daarbij helaas vaak over het hoofd gezien.
In dit artikel geef ik tips hoe je mensen meer bewust maakt op dit gebied.

Oorzaak: een menselijke fout

Bij ongelukken lezen we het vaak: de oorzaak is een menselijke fout. Bij Informatiebeveiliging is dit niet anders, het merendeel van de incidenten wordt veroorzaakt door menselijk handelen.
Je kunt de organisatorische en technische beveiliging in je organisatie nog zo goed op orde hebben als jouw (ingehuurde) medewerker een onbeveiligde laptop bij een klant achterlaat (KPN) is je hele beleid in één klap waardeloos.
Als de medewerker een boodschappenlijstje maakt op de achterkant van een dienstoverdracht en deze na de boodschappen achterlaat in het winkelwagentje (Haga ziekenhuis) zijn al de technische maatregelen nutteloos.
Een goed informatiebeveiligings- en privacy beleid (IBP-beleid) is een noodzakelijke voorwaarde. De technische maatregelen zijn voldoende voorwaarden maar de effectiviteit in de praktijk staat of valt met de mensen.
Met mensen die zich bewust zijn dat ze gegevens verwerken die privacygevoelig (kunnen) zijn, die zich bewust zijn van de risico's die zij en hun organisatie met betrekking tot deze gegevens lopen.

Aandachtspunten bij de ontwikkeling

- Bedenk wat het startpunt is

Kijk eerst welke volwassenheid de organisatie heeft op het gebied van privacy en informatiebeveiliging.
Is er een cultuur waarin medewerkers zich bewust zijn van IBP-risico's of is de cultuur meer gebaseerd op vertrouwen? We kennen elkaar toch, dus het is gewoon handig dat we de wachtwoorden voor onze email met elkaar delen.
Stem je acties af op de mate van volwassenheid van de organisatie. Een organisatie met een hoog bewustzijn vraagt om andere acties dan eentje waar IBP nog in de kinderschoenen staat.
Let bij grotere organisaties ook op of het privacy bewustzijn overal hetzelfde is. Vaak is het management, in AVG-termen: de verwerkersverantwoordelijke, doordrongen van de noodzaak, maar dat betekent nog niet dat het onderwerp op de werkvloer leeft.

- Geen eenmalige actie maar een programma

Herhaal de boodschap in verschillende vormen op verschillende tijdstippen. Maak daarom op basis van de inventarisatie een programma. Wanneer plannen we een actie en in welke vorm? Met een programma voorkom je dat acties er in de hectiek van alle dag bij inschieten.
Pas daarbij een mix van communicatiekanalen toe. Gebruik zowel bestaande als nieuwe communicatiekanalen. Benut de nieuwsbrief voor het personeel om IBP onder de aandacht te brengen. Vraag tijdens een personeelsbijeenkomst podium en vertel over de nieuwe ontwikkelingen.
Wissel mondelinge en schriftelijke communicatie af. Sommige mensen lezen liever iets, anderen zijn meer auditief ingesteld. Om de boodschap zo breed mogelijk gedragen te krijgen spreek je beide groepen aan. Maak bijvoorbeeld een poster met privacy-tips en hang die op strategische plekken (koffie apparaat, kopieerder).
Betrek ook het online element in je programma. In de markt zijn voldoende e-learning applicaties die medewerkers aangeboden kunnen worden. Sommigen koppelen daar ook nog een toets met een certificaat aan.
Zet de medewerkers die het certificaat hebben behaald in het zonnetje tijdens een personeelsborrel.

Bewustwording is een gemeenschappelijke verantwoording

Het maken van IBP bewuste medewerkers is niet alleen een taak van de Information Security Officer (ISO) of de Data Protection Officer (DPO). Het dient een gemeenschappelijke inspanning te zijn, ook voor het management. Zij hebben een belangrijke voorbeeldfunctie: door het naleven van de regels onderschrijven zij impliciet het belang van de regels.
Richt het programma ook op de hele organisatie. Betrek ook medewerkers van bijvoorbeeld de facilitaire afdeling. Bedenk daarbij dat zij andere vragen en issues hebben dan de werkvloer.

DePrivacyGuru

Wij helpen je graag met een goede privacy verklaring voor je medewerkers of bij het ontwikkelen van een privacy bewustzijn programma.

Het ontwikkelen van een goed privacy bewustzijn programma kost veel tijd. Bovendien heb je daar didactische kennis en ervaring voor nodig.
En dan moet je ook nog eens "de planken op": je moet voor de groep gaan staan, de presentatie of training zelf geven. Misschien helemaal jouw "ding" niet.
Bovendien heb je altijd het risico van interne reputatieschade als de training niet naar wens verloopt.
Wij hebben verschillende standaard trainingen ontwikkeld. Na een intake gesprek waarin we doelen, beschikbare tijd, locatie, doelgroep en niveau van de training bespreken, maken we deze op maat voor jouw organisatie.
Ook voor grotere groepen geven wij graag een presentatie.

Waarom een externe training of presentatie?

- Ook trainen is een vak, als FG doe je dit naast je gewone taken
- Voorkomen van interne reputatieschade
- Tijdsbesparing: de basis is al ontwikkeld

Waarom een trainer van DePrivacyGuru?

- Ervaren trainers die hun werk als trainer vaak combineren met een docentschap
- Pragmatisch in hun benadering
- Gewend voor grote groepen te spreken

Meer informatie: www.deprivacyguru.nl

info@deprivacyguru.nl

085-2223232

DePrivacyGuru: "Privacy zonder gedoe"