Hunter Management Partners BV

Bezoekadres:
Lopikerplein 2a, Schoonhoven
2e etage "De Toren"

Postadres:
Postbus 9, 3410 CA Lopik

Tel: 0182 - 389036
Fax: 0182 - 389048
E-mail: hmp@hmp.nl
Web: www.hmp.nl
KvK Midden NL 53164946

CHECKLIST AVG

voor werkgevers inzake personeel

Wat dient u als werkgever voor 25 mei 2018, te hebben gedaan om persoonsgegevens van werknemers te verwerken conform de verplichtingen uit de AVG?

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG), ook wel de General Data Protection Regulation (GDPR) genoemd, in werking. De AVG is Europese wetgeving en werkt direct door in de gehele Europese Unie. De wetgeving is al vanaf 2016 van kracht. Tot 25 mei 2018 heeft men de tijd gehad om de wetgeving door te voeren. Vanaf 25 mei 2018 wordt dan ook verwacht dat je als organisatie voldoet aan de AVG.

Door de Autoriteit Persoonsgegevens kan een boete van maximaal 20 miljoen of 4% van de jaarlijkse wereldwijde omzet opgelegd worden, indien vastgesteld wordt dat de verplichtingen uit de AVG niet worden nageleefd. Daarnaast komt er een 'kliklijn' en zullen er meer controles plaatsvinden.

Met behulp van deze checklist kan worden nagegaan of u als werkgever voldoet aan de AVG wetgeving. Vragen of wilt u weten wat Hunter Management Partners voor u kunt betekenen betreffende de vernieuwde privacy wetgeving? *Neem contact op met mr. V.S. (Vera) Verlooij, junior partner en jurist bij HMP, via v.verlooij@hmp.nl.*

AVG en persoonsgegevens van werknemers

De AVG ziet toe op de verwerking van persoonsgegevens van natuurlijke personen. Gegevens van werknemers vallen onder persoonsgegevens.

Onder *persoonsgegevens* in de AVG wordt onder andere verstaan:

- Naam, adres, woonplaats;
- Telefoonnummer;
- E-mailadres;
- Bankgegevens.

Onder *bijzondere persoonsgegevens* wordt onder andere verstaan:

- Afkomst;
- Geaardheid;
- Medische gegevens;
- BSN-nummer;
- Paspoorten.

AVG STAPPENPLAN VOOR WERKGEVERS MET BETREKKING TOT PERSONEEL

Stap 1: Inventarisatie/ register van verwerkingsactiviteiten
Toelichting: Iedere werkgever heeft in de uitoefening van bedrijfsvoering te maken met de verwerking van persoonsgegevens van werknemers.

De eerste stap om te voldoen aan de AVG, is het bewust worden van de persoonsgegevens die u als werkgever verwerkt en hier een inventarisatie van te maken. Dit doet men in een register van verwerkingsactiviteiten.

Bij organisaties met meer dan 250 werknemers, is een register van verwerkingsactiviteiten verplicht. Een organisatie met minder dan 250 medewerkers moet over een register beschikken wanneer de organisatie persoonsgegevens verwerkt:

- Waarvan de verwerking niet incidenteel is. In de praktijk zijn verwerkingen zelden incidenteel;
- Die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt; en/of
- Die vallen onder de categorie bijzondere persoonsgegevens.

Of een verwerkingsactiviteitenregister al dan niet verplicht is, het bijhouden van een register van gegevensverwerking draagt bij aan uw *verantwoordingsplicht* en maakt het voldoen aan de overige AVG bepalingen een stuk gemakkelijker.

Een voordeel van het hebben van een verwerkingsactiviteitenregister is dat bij controle van de Autoriteit Persoonsgegevens u het register direct kunt laten zien en daarmee grotendeels voldoet aan uw verantwoordingsplicht.

Uitvoering:

In het verwerkingsactiviteitenregister wordt een inventarisatie gemaakt van de antwoorden op de volgende vragen:

- Welke persoonsgegevens van werknemers verzamelt de organisatie? (bijvoorbeeld, naam, telefoonnummer)
- Verzamelt de organisatie ook bijzondere persoonsgegevens? (BSN, NAW gegevens, pasfoto's, camerabeelden)
- Van wie worden persoonsgegevens verwerkt (personeel, sollicitanten e.d.)
- Zijn de personeelsleden op de hoogte van de verwerking?
- Met welk doel en met welke grondslag worden de persoonsgegevens verwerkt? (werving en selectie van personeel, personeelsbestand, personeelsadministratie, verplicht vanuit andere instanties zoals de Belastingdienst)
- Hoe lang bewaart de organisatie de gegevens?
- Wie binnen de organisatie verzamelt/verzamelen de persoonsgegevens?
- Wie binnen de organisatie heeft toegang tot de persoonsgegevens?
- Worden de persoonsgegevens gedeeld met andere (internationale) organisaties?
- Heeft de organisatie een Functionaris voor de Gegevensbescherming (FG)?
- Welke maatregelen heeft de organisatie genomen om persoonsgegevens die de organisatie verwerkt te beveiligen?

In de volgende stappen worden deze vragen nader toegelicht. De antwoorden dienen in het register te worden opgenomen.

Stap 2: Doel en grondslag voor de verwerking van persoonsgegevens

Toelichting:

Het verwerken van persoonsgegevens mag enkel plaatsvinden voor een *gerechtvaardigd doel* (doelbinding). Enkel de persoonsgegevens die noodzakelijk zijn voor het bereiken van dit doel, mogen worden verzameld. Doel is bijvoorbeeld: identificatie, werving van personeel of personeelsadministratie.

Let op dat er niet meer persoonsgegevens worden verzameld dan nodig.
Voorbeeld: identificatieplicht. Veelal wordt om te voldoen aan de identificatieplicht een kopie gemaakt van het paspoort. Maar er zou ook een vinkje gezet kunnen worden: ID gezien, met het documentnummer. Hetzelfde doel, veel minder persoonsgegevens.

Gegevens die verkregen zijn voor een bepaald doel, mogen niet gebruikt worden voor andere doeleinden. Een e-mailadres ontvangen via een contactformulier, mag niet zonder toestemming op de nieuwsbrieflijst geplaatst worden.

Als het doel is vastgesteld, moet vervolgens de *grondslag* bepaald worden.
Verwerking van persoonsgegevens mag alleen als er sprake is van 1 van de 6 grondslagen die zijn opgenomen in de AVG.
De grondslagen zijn:

1. *Uitvoering van de overeenkomst*: er is een overeenkomst tussen de verwerker en de betrokkene en voor deze overeenkomst is het verwerken van een aantal persoonsgegevens onontbeerlijk. Bijvoorbeeld: de persoonsgegevens in de arbeidsovereenkomst of de bankgegevens om uitvoer te geven aan de overeengekomen loonbetaling.
2. *Wettelijke verplichting*: hieronder vallen de verwerkingen waarvoor geldt dat het niet mogelijk is om een wettelijke plicht uit te voeren, zonder de verwerking van persoonsgegevens. Bijvoorbeeld: gegevens in de HR-administratie. Bepaalde gegevens zijn noodzakelijk voor wettelijke verplichtingen zoals het betalen van belastingen en premies.
3. *Toestemming*: de organisatie verwerkt alleen persoonsgegevens na toestemming van de betrokkene. De toestemming moet een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting bevatten.
   Een mededeling zoals: bij gebruik gaat u akkoord, is geen toestemming. Het personeelslid moet echt een handeling van toestemming verrichten, zoals een checkbox aanvinken of wel of niet akkoord geven. Toestemming is bijvoorbeeld benodigd voor het verzamelen van foto's en gegevens voor het interne "smoelenboek".
   Binnen een organisatie geeft de grondslag toestemming nog een probleem. Bij toestemming mag er geen enkele sprake zijn van hiërarchie of machtsverhouding. Voor toestemming mag er derhalve geen enkele dwang vanuit de werkgever bestaan. Het beste kan er om de toestemming heen gewerkt worden. Geen toestemming vragen maar de keus bij de werknemer te laten.
4. *Gerechtvaardigd belang*: in de AVG worden de volgende voorbeelden gegeven: ten behoeve van direct marketing, het doorsturen van personeelsgegevens tussen verschillende onderdelen van het concern, het verzamelen van gegevens ten behoeve van netwerkbeveiliging.
   De vraag die bij een gerechtvaardigd belang gesteld moet worden: is het voor de betrokkene, het personeelslid, logisch dat zijn gegevens verzameld en verwerkt worden: reasonable expectancy of privacy.
5. *Vitaal belang*: komt binnen de organisatie niet veel voor. Bij vitaal belang is gegevensverwerking gerechtvaardigd ter bestrijding van ernstig gevaar voor de gezondheid van de betrokkene of een ander persoon. Het verzamelen van bepaalde gegevens van personeel kan een vitaal belang hebben; indien de werknemer lijdt aan bijvoorbeeld epilepsie of een bepaalde ernstige allergische reactie kan hebben. Het is daarbij van vitaal belang voor de werknemer dat de werkgever op de hoogte is van deze toestand, zodat indien nodig, de juiste acties genomen kunnen worden.
6. *Algemeen belang of openbaar gezag*: bestemd voor overheidsinstanties.

Uitvoering:

1. Rangschik het overzicht van verzamelde persoonsgegevens naar categorie. Bijvoorbeeld arbeidsovereenkomst, salarisadministratie e.d.
2. Geef per categorie aan welke gegevens worden verzameld.
3. Geef per categorie aan welk gerechtvaardigd doel en welke grondslag aan de basis ligt.

Stap 3: Gegevensbeschermingsbeleid ofwel privacy beleid (anders dan privacyverklaring!) & rechten van werknemers

Toelichting:

Privacy beleid

Een privacy beleid is voor een organisatie verplicht als dit in verhouding staat tot de verwerkingsactiviteiten. Dit is afhankelijk van de aard, omvang, context en doel van de gegevensverwerking. Het komt er op neer dat een privacy beleid alleen hoeft te worden opgesteld als er veel en/of bijzondere persoonsgegevens worden verzameld en verwerkt. De AVG werkt de vereisten verder niet uit.

Wederom, ook al is het opstellen van een privacy beleid voor veel organisaties niet verplicht, is het wel ten zeerste aan te bevelen. Personeelsleden moeten immers geïnformeerd worden over de verzameling en verwerking van hun persoonsgegevens (de verantwoordingsplicht). Maar ook intern is een beleid uitermate handig. Het opstellen van een privacy beleid zorgt ervoor dat de privacy van betrokkenen gewaarborgd wordt en binnen de organisatie is duidelijk hoe er met privacy omgegaan wordt. In plaats van een apart privacy beleid voor werknemers, kan er natuurlijk ook een hoofdstuk opgenomen worden in het personeelshandboek/reglement.

In het privacy beleid wordt onder andere het volgende qua personeel opgenomen:
Welke gegevens wordt er over personeel verzameld, hoe lang, waar, door wie, waarom?
Kunnen de gegevens ingezien worden? Waar kunnen klachten ingediend worden? Kunnen de gegevens verwijderd worden, wat zijn de rechten van de werknemers met betrekking tot de persoonsgegevens?

Rechten van werknemers

Onder de AVG hebben betrokkenen en dus ook werknemers een aantal nieuwe rechten met betrekking tot de persoonsverwerking verworven. Volgens de AVG is de werkgever verplicht de werknemer te informeren over deze rechten:

1. Dataportabiliteit: werknemers hebben het recht om hun dossier mee te nemen naar een nieuwe werkgever. De werkgever moet dit mogelijk maken. Let er daarom op dat de personeelsdossiers op orde zijn en geen onnodige informatie bevatten.
2. Recht van inzage: De werknemer heeft het recht om zijn personeelsdossier in te zien.
3. Recht van correctie: De werknemer heeft het recht om een correctieverzoek in te dienen voor gegevens die: feitelijk onjuist zijn, onvolledig zijn, niet ter zake doen of op een andere manier in strijd zijn met de wet.

Tip: neem in het persoonsreglement/handboek een hoofdstuk over de AVG en het privacy beleid op.

Uitvoering:

In het privacy beleid moet het volgende worden opgenomen:

- Het doel en de grondslag voor de verwerking van de persoonsgegevens;
- Dat de werkgever erop toeziet dat iedere verwerking van persoonsgegevens voldoet aan dit doel;
- Dat de verwerking niet verder gaat dan noodzakelijk;
- Dat de persoonsgegevens niet voor een ander doel worden gebruikt;
- Hoe men binnen de organisatie omgaat met persoonsgegevens;
- Hoe de werknemer een klacht in kan dienen;
- De rechten van de werknemers met betrekking tot de persoonsgegevens.

Stap 4: privacy by design en privacy by default

Toelichting:
Privacy by design; bij het ontwerpen van nieuwe producten en/of diensten moet *vooraf* een inschatting gemaakt worden van de privacy impact en hoe u er voor zorgt dat de persoonsgegevens goed beschermd worden.

Privacy by default; bij bestaande producten en/of diensten dient u technische en organisatorische maatregelen te treffen die ervoor zorgen dat de privacy van persoonsgegevens gewaarborgd worden.

Voorbeelden:
- Niet meer gegevens verzamelen dan nodig is voor het doel (denk aan gegevens voor de nieuwsbrief, vraag niet meer gegevens dan nodig is om de nieuwsbrief te versturen);
- Bewaartermijnen: bewaar gegevens niet langer dan wettelijk vastgelegd en/of noodzakelijk;
- Checkboxen op de website niet vooraf aanvinken;
- Doelbinding: verkregen persoonsgegevens enkel gebruiken voor het verkregen doel (denk aan e-mailadressen verkregen door weggevers op de website, niet gebruiken voor de nieuwsbrief);
- Beveiliging van de gegevens: beperk de toegang, beveilig de toegang.

Uitvoering:
Voor de relatie werkgever en werknemer bestaat de privacy by default voornamelijk uit:
1. De bewaartermijnen bepalen van de gegevens van de werknemers;
2. Het beveiligen van de persoonsgegevens;
3. Bepalen wie er toegang hebben tot de personeelsgegevens;
4. De huidige personeelsdossiers opruimen; onnodige persoonsgegevens verwijderen (lees recht op data portabiliteit) en de bewaartermijnen nalopen.

De bewaartermijnen zijn als volgt:
- Kopieën van identiteitsbewijzen: verwijderen op moment van uitdiensttreding (met uitzondering kopie ID voor loondossier: 5 jaar na uitdiensttreding);
- Overige personeelsdocumenten: verwijderen maximaal 2 jaar na uitdiensttreding;
- Uitzondering: gegevens die betrekking hebben op de bewaarplicht van de Belastingdienst (fiscale waarde, van waarde voor de loonbelasting): 7 cq. 5 jaar.
- Loonbeslagen: direct verwijderen na afloop;
- Functioneringsverslagen: 2 jaar na uitdiensttreding.

Let op: het gebruiken van het BSN-nummer als personeels- of dossiernummer is niet toegestaan.

Privacy by design komt aan de orde bij bijvoorbeeld de aanschaf van nieuwe verzuimregistratie software. Daarbij kunnen dezelfde stappen worden doorlopen als privacy by default. Enkel moet de uitkomst van de stappen bepalend zijn of de nieuwe software voldoet aan de privacy vereisten.

Stap 5: Functionaris Gegevensbescherming (FG)

Toelichting:
De Functionaris Gegevensbescherming (FG) is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.
De FG is in 3 situaties verplicht:
1. Overheden en publieke organisaties: Overheidsinstanties en publieke organisaties zijn altijd verplicht een FG aan te stellen. (gemeente, provincie, zorg- en onderwijsinstellingen)
2. Observaties: Organisaties die als hoofdtaak hebben: het op grote schaal volgen van individuen. Denk hierbij aan profilering van mensen en cameratoezicht. (beveiligingsmaatschappijen, marketingactiviteiten op basis van gegevens, risicobeoordeling, telecommunicatie)

3. Bijzondere persoonsgegevens: Organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waarvan dit de hoofdtaak is. (verzekeringsmaatschappij, bank) Niet vallen hieronder de eenpitters (de individuele arts of advocaat).

Een en ander zal in de toekomst nader opgehelderd worden. Er zal een lijst vanuit de Autoriteit Persoonsgegevens volgen, met daarin richtlijnen over op welke organisaties de verplichting van een FG rust. Advies voor nu is: wanneer onduidelijk is of uw organisatie verplicht is om een FG aan te stellen, onderbouw goed waarom wel of niet gekozen is voor het aanstellen van een FG.

Het vrijwillig aanstellen van een FG is toegestaan. Een FB mag iemand intern of extern in de organisatie zijn.

Uitvoering:

1. Bepaal of het aanstellen van een FG noodzakelijk is;
2. Onderbouw deze keuze zorgvuldig;
3. Meld de FG aan bij de Autoriteit Persoonsgegevens via het webformulier;
4. Geef aan de werknemers door wat het takenpakket is van de FG en hoe de FG te bereiken is (bijvoorbeeld in het privacy beleid)

Stap 6: DPIA, data protection impact assessment, gegevensbeschermingseffectbeoordeling

Toelichting:

De DPIA is een instrument om vooraf privacy risico's van een gegevensverwerking in kaart te brengen en om vervolgens maatregelen te treffen om deze risico's te verkleinen.

De DPIA is enkel verplicht voor organisaties en verwerkingen met een groot privacy risico voor de betrokkenen (diegene van wie de gegevens worden verzameld). Hiervoor gelden dezelfde criteria als onder stap 5. Denk aan profilering en prognoses op basis van kenmerken zoals, iemands beroepsprestaties, interesses, locatie, kredietwaardigheid, het volgen van websitebezoekers, automatische vacature selectie enz.

Bij het gebruik van nieuwe technologieën is een DPIA in ieder geval verplicht.

Eveneens zal in de toekomst een gemeenschappelijke EU-lijst van verwerkingen waarvoor een DPIA verplicht is, ter beschikking worden gesteld.

Een bedrijf dat stelselmatig de activiteiten van zijn werknemers monitort, inclusief hun werkplek, internetactiviteit enz., is verplicht tot een DPIA.

Uitvoering:

1. Bepaal als organisatie of een DPIA verplicht is;
2. Zo ja, voer de beoordeling uit volgens de richtlijnen van de Autoriteit Persoonsgegevens.

Stap 7: Datalek, beleid en datalekregister

Toelichting:

Melden datalek binnen 72 uur

Sinds 2016 geldt er een meldplicht voor datalekken. Deze meldplicht houdt in dat organisaties een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In een aantal gevallen moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Een datalek levert niet per definitie een boete op; het niet melden van een datalek kan daarentegen wel een boete opleveren.

Definitie datalek
Datalek: Er heeft een beveiligingslek plaatsgevonden. Bij dit beveiligingsincident zijn persoonsgegevens verloren gegaan en/of is onrechtmatige verwerking van deze persoonsgegevens niet uit te sluiten. (Denk aan diefstal computer, inbraak hacker, kwijtraken USB stick en brand).
Het ongeoorloofd wijzigen, inzien of verstrekken van gegevens, is ook een datalek.
Gegevens van een werknemer die per ongeluk terecht komen in het personeelsdossier van een collega is ook een datalek.

Melding datalek Autoriteit Persoonsgegevens: Gaat het om een datalek waarbij persoonsgegevens van gevoelige aard, of als er om een andere reden sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, meld deze dan zo spoedig mogelijk maar binnen uiterlijk 72 uur aan de Autoriteit Persoonsgegevens.

Melding datalek betrokkenen: Waren niet alle gelekte gegevens (correct) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene, dan dient het lek gemeld te worden aan de betrokkenen.

Voor de werkgever zijn voorbeelden van de aard van datalekken die gemeld moet worden:
- Gegevens over de gezondheid;
- Lidmaatschap vakvereniging
- Financiële gegevens en/of situaties zoals salaris –en betaalgegevens en schulden;
- Documentatie van functionering op werk;
- Eventuele persoonlijke problemen van werknemers (verslaving e.d.)
- Gebruikersnamen, inloggegevens en wachtwoorden;
- Kopieën identiteitsbewijzen en/of Burgerservicenummer.

Uitvoering:
1. Stel een datalek beleid op.
- Maak het voor de werknemers duidelijk wat een datalek is en hoe deze intern gemeld moet worden en bij wie.
- Stel een stappenplan datalek op. Datalekken moeten zo spoedig mogelijk maar uiterlijk binnen 72 uur gemeld worden.
2. Stel een datalekregister op: alle datalekken binnen de organisatie moeten worden vastgelegd in een register. Hierin moet worden opgenomen:
- Het soort gegevens
- Een omschrijving van het datalek
- Wanneer het datalek plaats vond;
- Wat er met de persoonsgegevens gebeurd is;
- Van welke personen gegevens gelekt zijn;
- Of er melding gemaakt is van het datalek
- Binnen hoeveel uur het datalek gemeld is.

Stap 8: Verwerkingsovereenkomsten

Toelichting:
Als een organisatie gegevensverwerking uitbesteed, dient met deze verwerker een verwerkingsovereenkomst opgesteld te worden.

Een verwerker is een persoon of organisatie die in opdracht van jou werkt met jouw verzamelde persoonsgegevens maar niet zelfstandig verantwoordelijk is voor de verwerking van de persoonsgegevens (over deze gegevens geen beslissingen mag maken). Denk aan de salarisadministratie, software, hosting partijen, (Cloud) opslag e.d. *Vereisten verwerkingsovereenkomst:* 1. Algemene beschrijving: duur, aard en doel van de verwerking; 2. Beschrijving van het soort persoonsgegevens, de categorieën gegevens; 3. Instructies verwerking: bepaling doeleinden verwerking; 4. Geheimhoudingsplicht; 5. Beveiliging; 6. Sub verwerkers; 7. Privacy rechten; 8. Melden datalekken; 9. Verwijderen gegevens na afloop verwerkingsdiensten; 10. Meewerken aan audits/controles
<u>Uitvoering:</u> 1. Maak een overzichtslijst van alle derden die u inhuurt voor de verwerking van persoonsgegevens. 2. Stel met iedere verwerker een verwerkingsovereenkomst op of inventariseer of deze door de verwerker zelf beschikbaar is gesteld. 3. Documenteer de lijst met verwerkers en de bijbehorende verwerkingsovereenkomsten.

Disclaimer
Hunter Management Partners heeft zijn best gedaan om zich zo goed mogelijk te verdiepen in de nieuwe wetgeving en de regels zo helder mogelijk aan u uit te leggen. Desondanks kan het zijn dat er onverhoopt toch onjuiste of onvolledige informatie in deze checklist is geslopen. Zie u iets dat niet klopt of niet duidelijk is? Laat het ons weten via hmp@hmp.nl of telefonisch 0182-389036