XpertHR

Welkom bij het XpertHR College,

met Steffie Schepers

Nieuwe Privacywet

In 10 stappen voorbereid op de AVG

XpertHR College

XpertHR

Mijn persoonsgegevens

Mr. Steffie Schepers
Advocate Arbeidsrecht

Fullservice: vastgoed en bestuursrecht, huurrecht, arbeidsrecht, familierecht, letselschade, privacyrecht, insolventie- en ondernemingsrecht

RWV ADVOCATEN

XpertHR

XpertHR College

Programma

- Wat is de AVG?
- Wat brengt de AVG?
- Wanneer is sprake van het verwerken van persoonsgegevens?
- Hoe implementeren we de AVG (doorlopen stappenplan)?
- Conclusie
- Vragen?

Wat is de AVG?

- AVG= Algemene Verordening Gegevensbescherming
- Nu nog: Wet Bescherming Persoonsgegevens (Wbp)
- Wbp is Nederlandse uitwerking van een uit 1995 daterende Europese privacyrichtlijn
- Per 25 mei 2018 vervangt de AVG de Wbp
- De AVG is een Europese Verordening die rechtstreeks doorwerkt en dus in de hele Europese Unie zal gaan werken
- Naast AVG, Uitvoeringswet Algemene verordening gegevensbescherming (op dit moment nog wetsvoorstel). Wet geeft nationale regels om AVG uit te voeren en regelt intrekking Wbp

Wat brengt de AVG?

- AVG geeft (net als Wbp) regels ten aanzien van het verwerken van persoonsgegevens
- AVG kent ten opzichte van Wbp:
  - versterking en uitbreiding van privacyrechten voor betrokkenen;
  - geeft organisaties meer verantwoordelijkheden en verplichtingen;
  - geeft alle Europese privacytoezichthouders (voor Nederland de Autoriteit Persoonsgegevens) dezelfde stevige bevoegdheden.

Wat is een persoonsgegeven? (I)

- Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon.
- Dit betekent dat informatie ofwel direct over iemand gaat (direct identificeerbaar), ofwel naar deze persoon te herleiden is (indirect identificeerbaar).
- Een natuurlijk persoon: dus gegevens van overleden personen of van organisaties zijn geen persoonsgegeven.
- Het gaat niet alleen om informatie over iemand in geschreven tekst, maar ook over beeld en geluid.

Wat is een persoonsgegeven? (II)

<u>Voorbeelden van persoonsgegevens:</u>

iemands naam, adres en woonplaats, geboortedatum, telefoonnummer, maar ook postcodes met huisnummers, emailadressen, bankrekeningnummers en IP-adressen, stemmen, vingerafdrukken, DNA-profiel of uiterlijke, sociale en/of economische kenmerken kunnen persoonsgegevens zijn.

Gegevens die ook maar enig verband (kunnen) hebben met levende mensen, zijn al snel ‘persoonsgegevens’ of kunnen dat worden.

Tip: ga er bij twijfel van uit dat het om een persoonsgegeven gaat.

Wat is een persoonsgegeven? (III)

De AVG maakt onderscheid tussen ‘gewone’ en ‘bijzondere’ persoonsgegevens. Deze laatste zijn gegevens over iemands:

- godsdienst of levensovertuiging;
- ras;
- politieke voorkeur;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakbond;
- strafrechtelijk verleden.

Voor deze verwerking gelden zwaardere eisen. Verwerking is verboden, tenzij daarvoor in de wet een uitzondering is opgenomen of uitdrukkelijk toestemming is gegeven door de betrokkene.

Wanneer spreek je van verwerken?

Onder het verwerken vallen alle handelingen die uitgevoerd kunnen worden met persoonsgegevens.

Het betreft dus een zeer ruim begrip (!) waaronder in ieder geval valt:

het verzamelen, vastleggen, opslaan, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorsturen, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en het vernietigen van gegevens.

Let op: bijna iedere verwerkingshandeling valt onder begrip verwerken in de zin van de AVG!

Implementatie AVG; Volg ons stappenplan!

STAP 1
Bepaal of u een functionaris voor de gegevensbescherming dient aan te stellen

STAP 2
Breng in kaart welke persoonsgegevens u verwerkt

STAP 3
Bepaal of u verplicht bent een Data Protection Impact Assessment uit te voeren

STAP 4
Stel een privacybeleid op

STAP 5
Maak een register verwerkingen en register datalekken

STAP 6
Stel vast wat uw doel is en wat de grondslag is voor de gegevensverwerking

STAP 7
Evalueer de manier waarop u toestemming vraagt, krijgt en registreert

STAP 8
Stel de wijze vast waarop informatie wordt verschaft aan de betrokkene

STAP 9
Controleer uw bewerkersovereenkomsten en verwerkersovereenkomsten

STAP 10
Bepaal onder welke toezichthouder u valt

Is uw organisatie al voorbereid op de AVG?

1. Ja, wij hebben de voorbereidingen afgerond
2. Wij zijn bezig met de voorbereidingen
3. Nee, wij hebben nog niets gedaan

STAP 1

Bepaal of u een functionaris voor de gegevensbescherming dient aan te stellen

Wel of niet verplicht FG aan te stellen

- Onder AVG kan de verplichting bestaan een functionaris voor de gegevensverwerking (FG) aan te stellen.
- FG = iemand die binnen organisaties toezicht houdt op op adviseert over de toepassing en naleving van AVG.
- Verplichting geldt voor organisaties die:
  - een overheidsinstantie of overheidsorgaan zijn; en/of
  - vanuit hun kerntaak op grote schaal individuen regelmatig en stelselmatig observeren (denk aan reisgegevens die worden bijgehouden door vervoersorganisatie); en/of
  - zich vanuit hun kerntaak bezig houden met het op grote schaal verwerken van bijzondere persoonsgegevens (denk aan ziekenhuizen/onderzoekinstellingen die gebruik maken van gezondheidsgegevens).
- Voor veel organisaties geldt de verplichting niet! Organisaties mogen vrijwillig FG aanstellen.

STAP 2
Breng in kaart welke persoonsgegevens u verwerkt

Welke persoonsgegevens worden verwerkt?

Achterhaal:

- welke gegevens worden verwerkt (maak hierbij onderscheid in gewone en/of bijzondere gegevens);
- van wie de gegevens zijn (bijv. van klanten, werknemers, leveranciers, bezoekers);
- door wie verwerking plaatsvindt (alleen door werknemers of verwerken anderen ook); en
- of deze gegevens met derden worden gedeeld (bijv. aan andere leveranciers of opdrachtnemers).

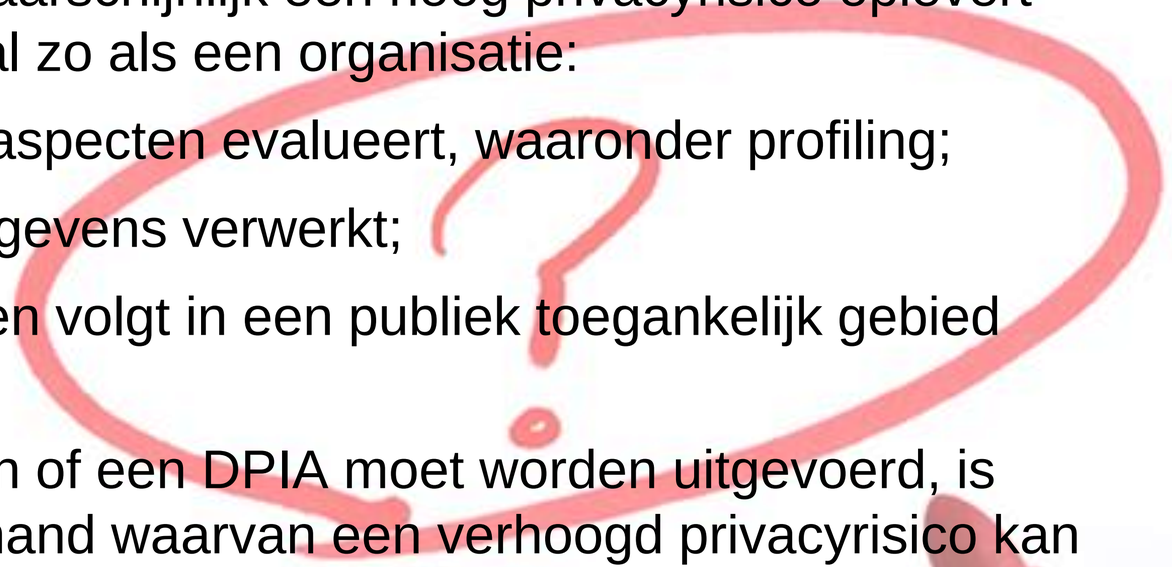
Deze informatie 1) helpt bewust te worden van de verwerkingen die plaatsvinden, 2) helpt inschatten wat de impact van de AVG is en welke aanpassingen nodig zijn om aan de AVG te voldoen en 3) vormt de basis voor de uitvoering van de volgende stappen.

STAP 3

Bepaal of u verplicht bent een Data Protection Impact Assessment uit te voeren

Wel of geen DPIA uitvoeren?

- DPIA = instrument in kaart brengen privacyrisico's om vervolgens deze risico's te verkleinen.
- Nederlandse naam: gegevensbeschermingeffectbeoordeling
- Verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. Dat is in ieder geval zo als een organisatie:
  - systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
  - op grote schaal bijzondere persoonsgegevens verwerkt;
  - op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).
- Om organisaties te helpen bij het bepalen of een DPIA moet worden uitgevoerd, is een lijst opgesteld van 9 criteria aan de hand waarvan een verhoogd privacyrisico kan worden vastgesteld.



STAP 4
Stel een privacybeleid op

Stel een privacybeleid op!

- Een privacybeleid is een intern document. Het is het beleid van de organisatie gericht tot iedereen die binnen en namens de organisatie werkt met persoonsgegevens.
- Een verplichting tot het opstellen, bestaat formeel alleen als beleid nodig is in verhouding tot verwerkingsactiviteiten.
- Maar: iedere organisatie heeft verantwoordingsplicht! Aangetoond moet worden dat de verwerkingen die plaatsvinden aan de regels van de AVG voldoen.
- Beleid zorgt ervoor dat aan deze verplichtingen kan worden voldaan, dus ons advies: DOEN!

Inhoud privacybeleid? (I)

Wat kan onderdeel uitmaken van een privacybeleid?

1. <u>Een dataminimalisatiebeleid</u>
   Organisatie is verplicht niet meer gegevens te verwerken dan nodig (bijvoorbeeld niet: politieke voorkeur, favoriete voetbalclub).
2. <u>Het Beveiligingsbeleid.</u>

   Hierin staan de beveiligingsmaatregelen die de organisatie neemt, zoals alarminstallatie op pand, firewall, wachtwoorden periodiek wijzigen etc., maar ook duidelijke afspraken wie binnen de organisatie toegang heeft tot persoonsgegevens.

Inhoud privacybeleid? (II)

3. Beleid datalekken.

- Hierin staat hoe de organisatie en de medewerkers moeten omgaan met een datalek.
- Datalek = beveiligingsincident dat leidt tot de vernietiging, wijziging of het vrijkomen van persoonsgegevens zonder dat dit de bedoeling is van deze organisatie.
- Bijvoorbeeld: klantenlijst in de trein laten liggen, maar ook: e-mail met klantgegevens naar verkeerde adres.
- Voorbeeld beleid: instructie steeds melden bij bepaalde medewerker, steeds incidentenformulier invullen, datalek registreren in register datalekken (dit is altijd verplicht), bepaalde medewerker beslist of gemeld wordt bij de AP en of betrokkene wordt geïnformeerd.

Inhoud privacybeleid? (III)

4. <u>Beleid omtrent de rechten van betrokkenen</u>.
   Daarin staat hoe u omgaat met de rechten van betrokkenen.
   Denk aan:
   - recht op informatie;
   - recht op inzage;
   - recht op correctie als gegeven niet kloppen;
   - recht op gegevenswissing; onder andere wanneer (i) de gegevens zijn niet langer nodig, (ii) betrokkene trekt de toestemming in, (iii) persoonsgegevens worden onrechtmatig verwerkt.
   - recht op beperking van de verwerking;
   - recht op gegevensoverdraagbaarheid (dataportabiliteit).

Dus: hoe worden (potentiële) werknemers over hun rechten geïnformeerd? Wat wordt gedaan als een werknemer een recht wil uitoefenen?

STAP 5
Maak een register verwerkingen en register datalekken

Opstellen register verwerkingen

- De AVG kent voor veel organisaties de verplichting een register verwerkingen op te stellen.
- Register verwerkingen = opsomming van belangrijkste informatie over de verwerkingen van persoonsgegevens
- Wanneer?
  - o.a. bij het hebben van 250 of meer medewerkers in dienst; en/of
  - bij het niet incidenteel verwerken van persoonsgegevens
- Conclusie: bijna iedere organisatie moet een register bijhouden!

Inhoud register verwerkingen (I)

Het register moet de volgende informatie bevatten:

- naam en contactgegevens van de organisatie;
- verwerkingsdoelen. Denk aan werving en selectie personeel, salarisbetaling
- beschrijving van de categorieën
  - betrokkenen (bijv. personeel en sollicitanten)
  - persoonsgegevens (bijv. NAW gegevens, telefoonnummer, e-mailadres, BSN)
  - ontvangers aan wie persoonsgegevens worden verstrekt (bijv. loonadministrateur)

Inhoud register verwerkingen (II)

Indien mogelijk/van toepassing:

- datum/termijn waarop gegevens moeten worden gewist
- algemene beschrijving van technische en organisatorische beveiligingsmaatregelen
- naam/contactgegevens partijen waarmee organisatie gezamenlijk verwerkingsverantwoordelijke is
- contactgegevens FG

Opstellen register datalekken

- De AVG kent verplichting een register datalekken bij te houden.
- Register datalekken = document waaruit blijkt welke datalekken zich in de organisatie hebben voorgedaan
- Datalekken moeten altijd geregistreerd worden in een intern register datalekken.
- Of gemeld moet worden bij de AP (binnen 72 uur) en bij de betrokkene(n) hangt af van de vraag of de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van de betrokkene(n).

STAP 6

Stel vast wat uw doel is en wat de grondslag is voor de gegevensverwerking

Stel vast wat het doel is (I)

- Verwerking van persoonsgegevens is alleen toegestaan voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel
- Welbepaald: doel is bepaald voorafgaand de verwerking en de doelomschrijving is voldoende duidelijk
  - Bijvoorbeeld: salarisbetaling
- Uitdrukkelijk omschreven: vermeldt het doel in het register verwerkingen (zie stap 5)
- Gerechtvaardigd: komt tot uitdrukking in de grondslag
- Zijn gegevens eenmaal voor een bepaald doel verzameld, dan mogen ze ook voor andere doelen worden gebruikt tenzij dat andere doel onverenigbaar is met het doel waarvoor de gegevens zijn verzameld

Stel vast wat de grondslag is (II)

- Verwerking van persoonsgegevens is alleen toegestaan indien de verwerking kan worden gebaseerd op één van de zes grondslagen
- Mogelijke grondslagen voor verwerking:
  - uitvoering van een overeenkomst waarbij de betrokkene partij is: zoals ter uitvoering van de arbeidsovereenkomst
  - wettelijke verplichting: zoals verplichting kopie ID werknemer in loonadministratie
  - gerechtvaardigd belang. Sociale media profiel sollicitant controleren, drie punten waar rekening mee dient te worden gehouden (i) is het noodzakelijk voor de uitvoering van de baan, (ii) dient het profiel een zakelijk of persoonlijk doel, (iii) is de betrokkene geïnformeerd?
  - maar ook mogelijk: toestemming van de betrokkene (stap 7) / vitaal belang / algemeen belang

STAP 7

Evalueer de manier waarop u toestemming vraagt, krijgt en registreert

Evalueer de manier waarop toestemming wordt gevraagd, verkregen en geregistreerd

Strenge voorwaarden:

- Toestemming vereist een verklaring of een actieve handeling
  - Verklaring is in principe vormvrij, maar let op de organisatie moet kunnen aantonen dat zij een geldige toestemming heeft ontvangen
- Toestemming is alleen geldig als deze vrij, specifiek, geïnformeerd en ondubbelzinnig is gegeven
  - Toestemming is niet vrij gegeven als de betrokkene alleen gebruik kan maken van een bepaalde dienst, als hij toestemming geeft voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst
  - Let op bij machtsverhouding

Let op: een gegeven toestemming kan op ieder moment worden ingetrokken

STAP 8

Stel de wijze vast waarop informatie wordt verschaft aan de betrokkene

Informeer de betrokkene (I)

Wanneer persoonsgegevens worden verzameld moet de betrokkene worden geïnformeerd over onder andere:

- de naam en contactgegevens van de verantwoordelijke
- de contactgegevens van de FG (indien van toepassing)
- het doel en de rechtsgrond van de verwerking van de persoonsgegevens
- de bewaartermijn of de criteria ter bepaling van die termijn (niet langer dan nodig)
- de rechten van betrokkene, zoals: inzage (wat, waarom, aan wie) / correctie / gegevenswissing / beperking van de verwerking / overdracht (zie stap 4)

Informeer de betrokkene (II)

Hoe kan dat opgelost worden? Informeer de betrokkenen via een privacyverklaring:

- in of bij de arbeidsovereenkomst voor het personeel;
- op de website plaatsen bij de vacature voor sollicitanten.

STAP 9
Controleer uw bewerkersovereenkomsten en verwerkersovereenkomsten

Wanneer dient een verwerkersovereenkomst te worden gesloten?

- Met een derde die ten behoeve van de organisatie persoonsgegevens verwerkt, zonder dat die derde aan diens rechtstreekse gezag is onderwerpen
- Wie bepaalt waarom er persoonsgegevens worden verwerkt (doel) en hoe dat gebeurt (middelen)?
- Wel met: administratiekantoor of cloud-dienstverlener
- Niet met: arbodienst die in opdracht van de werkgever de re-integratie verzorgt
- Is een verplichting van zowel de verwerkingsverantwoordelijke als de verwerker

De verwerkersovereenkomst, wat moet daarin staan? (I)

- algemene beschrijving van de verwerkingsactiviteit (welke persoonsgegevens worden verwerkt, met welk doel, hoe lang, op welke manier?)
- dat persoonsgegevens alleen worden verwerkt onder de schriftelijke instructies van de verwerkingsverantwoordelijke;
- geheimhoudingsplicht van de verwerker;
- beveiliging verwerking;
- geen subverwerkers inschakelen zonder toestemming;
- datalekken;
- ondersteuning bieden bij het nakomen van de verplichtingen van de verwerkingsverantwoordelijke met het oog op de privacyrechten van betrokkenen;
- gegevens verwijderen bij einde overeenkomst;
- meewerken aan audits.

N.B. maak ook afspraken over de aansprakelijkheidsverdeling

STAP 10
Bepaal onder welke toezichthouder u valt

Bepaal de toezichthouder

- Het bepalen van de leidend toezichthouder is alleen relevant wanneer grensoverschrijdende verwerkingen van persoonsgegevens worden uitgevoerd.
- De leidend toezichthouder is in principe de toezichthouder van de lidstaat waar de organisatie is gevestigd. Zijn er meerdere vestigingen in de EU, dan moet bepaald worden welke vestiging de hoofdvestiging is.

Conclusie

Als organisatie (verwerkersverantwoordelijke) ben je verantwoordelijk en moet je aantonen dat de in de AVG opgenomen beginselen worden nageleefd.

De organisatie moet daarvoor onder andere:

- een aantal documenten opstellen, zoals een privacybeleid, register verwerkingen, register datalekken, privacyverklaring en verwerkersovereenkomst;
- onder bepaalde omstandigheden een FG aanstellen;
- in bepaalde gevallen een DPIA uitvoeren.

STAP 1
Bepaal of u een functionaris voor de gegevensbescherming dient aan te stellen

STAP 2
Breng in kaart welke persoonsgegevens u verwerkt

STAP 3
Bepaal of u verplicht bent Data Protection Impact Assessment uit te voeren

STAP 4
Stel een privacybeleid op

STAP 5
Maak een register verwerkingen en register datalekken

STAP 6
Stel vast wat uw doel is en wat de grondslag is voor de gegevensverwerking

STAP 7
Evalueer de manier waarop u toestemming vraagt, krijgt en registreert

STAP 8
Stel de wijze vast waarop informatie wordt verschaft aan de betrokkene

STAP 9
Controleer uw bewerkersovereenkomsten en verwerkersovereenkomsten

STAP 10
Bepaal onder welke toezichthouder u valt

Bekijk het stappenplan op onze website

Klik hier voor het stappenplan